Mathematisches Forschungsinstitut Oberwolfach

Report No. 37/2007

Permutation Groups

Organised by
Robert Guralnick, Los Angeles
Cheryl Praeger, Crawley
Jan Saxl, Cambridge
Katrin Tent, Bielefeld

August 5th – August 11th, 2007

Abstract.
The theory of permutation groups is essentially the theory of symmetry for mathematical and physical systems, and therefore has major impact in diverse areas of mathematics. Recent significant advances in permutation groups have contributed to, and benefited from, many areas, leading to a more powerful permutation group theory including astonishingly complete classifications and asymptotic results. The workshop brought together leading researchers in permutation groups with those from related disciplines.

Mathematics Subject Classification (2000): 20B, 20C, 20G, 03C, 05B, 05C, 05E, 12E99, 06B.

Introduction by the Organisers

The workshop *Permutation groups* organised by Robert Guralnick (Southern California), Cheryl Praeger (Western Australia), Jan Saxl (Cambridge) and Katrin Tent (Bielefeld) was held August 5th-11th, 2007. The focus was recent developments in permutation group theory and their influence on, and from, group representation theory, algebraic graph theory and other areas of geometry and combinatorics, algebraic geometry, model theory and infinite symmetrical structures. It was well attended with 50 participants.

Especially valuable was the program to support young researchers which gave the opportunity for a considerable number of young mathematicians to participate in the workshop. They benefited from the 'Oberwolfach experience' and also enlivened and contributed enormously to the success of the meeting.

The workshop had a friendly and vibrant atmosphere, aided by the excellent facilities of the Institute. All participants appreciated the beautiful lecture by John G. Thompson entitled 'The divisor matrix and $\mathrm{SL}(2,\mathbb{Z})$'. (In fact, this meeting was the first Oberwolfach workshop in over twenty years that Thompson had attended.) There were 26 other talks, and the program featured in each of the first five sessions at least one talk by a student or young researcher at the beginning of their career. This facilitated interaction between younger and more established researchers. The number of talks was restricted to give plenty of time for discussion and cooperation among the participants. Other communications were presented as posters.

Highlights of the workshop addressed both fundamental permutation group theory, and also significant outcomes from applying permutation group theory and methods in combinatorics, model theory and other areas. Some topics arose in more than one context, forming new connections. A common feature of many contributions was application of the finite simple group classification, or new results on the structure of simple groups. As examples, we mention two highlights reported by early career participants.

The question of base size of permutation actions is of importance in computational group theory as well as in the study of the graph isomorphism problem. Recent research has thrown much light on the base sizes of actions of almost simple groups in particular. Burness reported on the very recent proof of a conjecture of Cameron and Kantor dating from 1993 concerning non-standard permutation actions of almost simple groups: these are all primitive actions apart from actions of alternating and symmetric groups on subsets or partitions, and of classical groups on subspaces or pairs of complementary subspaces. In all the latter families the minimum base size is unbounded as the group order increases. The somewhat surprising conjecture, now proved, is that the minimum base size of non-standard permutation groups is at most 7, with the unique example where this bound is attained being the Mathieu group M_{24} in its natural action on 24 points.

Expander graphs play an important role in computer science and combinatorics, and, for example, are significant in modelling and analysing communication networks. In particular, their diameters grow only logarithmically with the numbers of vertices. This property on diameters was proved in 1989 by Babai, Kantor and Lubotzky to hold for suitable Cayley graphs of simple groups: specifically for each finite nonabelian simple group G, they constructed a valency 7 Cayley graph for G with diameter at most a constant times $\log(|G|)$. Although their graphs were not expanders, they conjectured that there exists an absolute constant k such that all infinite families of simple groups give rise to families of valency k Cayley graphs that are expanders. Kassabov lectured on amazing progress towards proving this conjecture – it is now proved for all simple groups apart from the Suzuki groups.

Other major areas discussed in lectures include the following:

- fundamental theory for families of transitive permutation groups, such as semi-primitive and extremely primitive groups;
- elements and subgroup structure of finite and algebraic groups;
- infinite permutation groups and automorphism groups of infinite structures;
- uses of permutation group methods in geometry and combinatorics, and geometric methods in group theory.

It was a very happy and successful workshop. Indeed, several of the most distinguished participants commented that this was one of the best Oberwolfach meetings they had attended, with plenty of time for collaboration, and outstanding talks.

Extended abstracts of the talks mentioned, as well as all the others, are given below (in the order in which they were presented).

Workshop: Permutation Groups

Table of Contents

Abstracts

Characters, mixing, covering and word maps

Aner Shalev

1. Character estimates in symmetric groups

The study of character values in symmetric groups is a challenging longstanding problem which, to a large extent, is still open. In the recent joint work [LaSh2] with Michael Larsen we provide bounds on $\chi(\sigma)$ for all $\chi \in \mathrm{Irr}(S_n)$ and all $\sigma \in S_n$, which are in many cases best possible.

In order to state the main result, define the *cycle growth sequence* of a permutation $\sigma \in S_n$ to be the sequence (b_k) such that that for every $k \geq 1$, σ has n^{b_k} cycles of length $\leq k$ (we set $b_k = 0$ if σ has no such cycles). Define

$$B(\sigma) = \sum_{k \geq 1} \frac{b_k}{k(k+1)}.$$

We can now state our main character-theoretic result.

Theorem 1.1. *For all $\epsilon > 0$ there exists N such that for all integers $n \geq N$, all permutations $\sigma \in S_n$, and all irreducible characters χ of S_n we have*

$$|\chi(\sigma)| \leqslant \chi(1)^{B(\sigma)+\epsilon}.$$

Theorem 1.1 has various interesting consequences, stated below.

Theorem 1.2. *Let $\sigma \in S_n$ and $\chi \in \mathrm{Irr}\, S_n$.*

(i) If σ is fixed-point-free, or has $n^{o(1)}$ fixed points, then $|\chi(\sigma)| \leq \chi(1)^{1/2+o(1)}$.

(ii) If m is a positive integer and σ has at most $n^{o(1)}$ cycles of length less than m, then $|\chi(\sigma)| \leq \chi(1)^{1/m+o(1)}$.

These bounds are best possible and generalize the Fomin-Lulov bound for permutations consisting of n/m m-cycles.

In the next result we bound all character values of σ in terms of the number of fixed points $\mathrm{fix}(\sigma)$ of σ.

Corollary 1.3. *Let $\sigma \in S_n$ and let $f = \max(\mathrm{fix}(\sigma), 1)$. Then for all $\chi \in \mathrm{Irr}(S_n)$ we have*

$$|\chi(\sigma)| \leq \chi(1)^{1-\frac{\log(n/f)}{2\log n}+o(1)}.$$

Our final result on character values uses the number of cycles as the main parameter.

Corollary 1.4. *Fix $\alpha \leq 1$ and let $\sigma \in S_n$ be a permutation with at most n^α cycles. Then for all $\chi \in \mathrm{Irr}(S_n)$ we have*

$$|\chi(\sigma)| \leq \chi(1)^{\alpha+o(1)}.$$

In the next sections we present applications of our character estimates to various classical problems.

2. Mixing

Random walks on finite (almost) simple groups G with respect to a conjugacy class C as a generating set have been studied extensively in the past decades. Our character estimates provide rather sharp bounds on the mixing time in A_n (see [LaSh2]).

Theorem 2.1. *For every positive integer t and a real number $\epsilon > 0$ there exists N such that if $n \geq N$ and $\sigma \in S_n$ satisfies $B(\sigma) \leq 1 - 1/t - \epsilon$, then $T(\sigma^{S_n}) \leq t+1$.*

This general result has various consequences.

Theorem 2.2. *Let $\sigma \in A_n$, and $C = \sigma^{S_n}$, and let $T = T(C, A_n)$ denote the mixing time of the associated random walk on A_n.*

(i) The mixing time T is bounded if and only if σ has at most n^{α} fixed points, where $\alpha < 1$ is bounded away from 1.

(ii) If $\alpha < 1$, $n \gg 0$, and σ has n^{α} fixed points, then

$$(1-\alpha)^{-1} \leq T \leq 2(1-\alpha)^{-1} + 1.$$

(iii) If σ is fixed-point-free or has $n^{o(1)}$ fixed points then $T \leq 3$.

(iv) If σ has at most $n^{o(1)}$ cycles of length 1 and 2 then $T = 2$.

Parts (iii) and (iv) are best possible, and extend results of Lulov.

In [Sh2] we obtain a somewhat surprising result for general (nonabelian) finite simple groups G, showing that the mixing time $T(G, C)$ is usually the smallest possible.

Theorem 2.3. *Let G be a finite simple group, let $x \in G$ be randomly chosen, and let $C = x^G$ be its conjugacy class. Then the probability that $T(C, G) = 2$ tends to 1 as $|G| \to \infty$. Consequently $|(x^G)^2|/|G| \to 1$ with probability tending to 1 as $|G| \to \infty$.*

Thus the square of a class of a random element of G covers almost all of G. This provides positive evidence towards a longstanding conjeture of Thompson, stating that every finite simple group G has a class C such that $C^2 = G$.

3. Covering

The study of covering simple groups by powers of classes has a long history. While Thompson's conjecture is still open for infinitely many simple groups, we show the following in [Sh1].

Theorem 3.1. *There exists an absolute constant c such that every finite simple group G of order $\geq c$ has a conjugacy class C such that $C^3 = G$. Furthermore, if $x \in G$ is randomly chosen, then the probability that $(x^G)^3 = G$ tends to 1 as $|G| \to \infty$.*

The case of symmetric and alternating groups is particularly interesting. On the one hand there are early results showing that $C^2 = A_n$ for certain classes C

(e.g. a class of an n-cycle). But very few classes like this have been found, and it remained open whether $C^2 = A_n$ is a rare or a common phenomenon.

In [LaSh2] we combine character methods with combinatorial constructions to show the following.

Theorem 3.2. *For any $\epsilon > 0$ there exists N such that if $n \geq N$ and $\sigma \in S_n$ consists of at most $(1/4 - \epsilon)n$ cycles, and has at most $n^{1/4-\epsilon}$ cycles of length 1 or 2, then $(\sigma^{S_n})^2 = A_n$.*

By the Erdős-Turán theory a random permutation in S_n has about $\log n$ cycles. Using the preceding theorem we can readily deduce the following.

Corollary 3.3. *Let $\sigma \in A_n$ be a randomly chosen permutation. Then the probability that $(\sigma^{A_n})^2 = A_n$ tends to 1 as $n \to \infty$.*

4. Word maps

By a *word* we mean an element $w = w(x_1, \ldots, x_d)$ of the free group F_d on $x_1, \ldots, x_d$. Given the word w we consider the *word map* $w_G : G^d \to G$ sending $(g_1, \ldots, g_d)$ to $w(g_1, \ldots, g_d)$. The set of all group elements of the form $w(g_1, \ldots, g_d)$ (where $g_i \in G$) is denoted by $w(G)$.

Word maps occur naturally in various contexts. A natural problem, which is a group theoretic version of Waring's problem in number theory, is to express group elements as short product of word values. In [Sh1] we prove the following somewhat surprising result.

Theorem 4.1. *For every word $w \neq 1$ there exists a number N such that if G is a finite simple group of order at least N then $w(G)^3 = G$.*

For example, every $g \in G$ can be written as a product of three kth powers, provided G is large enough. This shows that Waring-type problems sometimes have better solutions in non-commutative contexts.

Is Theorem 4.1 above best possible? In [LaSh1] and [LaSh2] we provide a stronger result for alternating groups.

Theorem 4.2. *For every word $w \neq 1$ there exists N such that if $n \geq N$ then $w(A_n)^2 = A_n$.*

The proofs rely on character bounds and many other tools, such as algebraic geometry and analytic number theory.

Finally, we pose the following.

Conjecture. *For any word $w \neq 1$ there is a number N such that if G is a finite simple group of order at least N then $w(G)^2 = G$.*

References

[LaSh1] M. Larsen and A. Shalev, Word maps and Waring type problems, Preprint, 2007.

[LaSh2] M. Larsen and A. Shalev, Characters of Symmetric groups: sharp bounds and applications, Preprint, 2007.

[Sh1] A. Shalev, Word maps, conjugacy classes, and a non-commutative Waring-type theorem, to appear in *Annals of Math.*

[Sh2] A. Shalev, Mixing and generation in simple groups, to appear in *J. Algebra.*

Geometric methods in group theory: Subgroups of linear groups over $\mathbb{F}_2$ generated by elements of order 3 with 2-dimensional commutator

Hans Cuypers

In his revision of Quadratic Pairs [2, 3], Chermak [2] classifies various subgroups of the symplectic groups $\mathrm{Sp}(2n,2)$ generated by elements d of order 3 with $[V,d]$ being 2-dimensional, where V is the natural module of $\mathrm{Sp}(2n,2)$. Besides the full symplectic group he encounters orthogonal and unitary groups over the field with 2 or 4 elements respectively, as well as alternating groups. Chermak's proof of his classification theorem is inductive and relies mainly on methods from geometric algebra.

By using discrete geometric methods as in [1, 4] we are able to classify subgroups of $\mathrm{GL}(V)$, where V is an $\mathbb{F}_2$-vector space of possibly infinite dimension, generated by elements d of order 3 with $[V,d]$ being 2-dimensional.

In particular, we prove the following.

Theorem. Let V be a vector space of dimension at least 3 over the field $\mathbb{F}_2$. Suppose $G \leqslant \mathrm{GL}(V)$ is generated by a conjugacy class D of elements of order 3 such that

- $[V,d]$ is 2-dimensional for all $d \in D$;
- $[V,G]=V$ and $C_V(G)=0$.

Then we have one of the following.

(i) There exists a subspace Φ of V^* annihilating V such that $G=\mathrm{T}(V,\Phi)$, i.e., the subgroup of $\mathrm{GL}(V)$ generated by all transvections whose axis is of the form $\ker(\phi)$ for some $\phi \in \Phi$. The class D is the unique class of elements of order 3 with 2-dimensional commutator on V.

(ii) $\dim(V)=3$ and $G=7:3$; D is one of the two classes of elements of order 3 in G.

(iii) $\dim(V)=4$ and $G \simeq \mathrm{Alt}_7$ (inside $\mathrm{Alt}_8 \simeq \mathrm{GL}(4,2)$); the class D corresponds to the class of elements of order 3 which are products of two disjoint 3-cycles inside Alt_7.

(iv) $\dim(V) \geq 6$, and $G=\mathrm{Sp}(V,f)$ with respect to some nondegenerate symplectic form on V; the class D is the unique class of elements of order 3 with 2-dimensional commutator on V.

(v) $\dim(V) \geq 6$ and G is isomorphic to $\Omega(V,q)$ for some nondegenerate quadratic form q on V. The class D is the unique class of elements of order 3 with 2-dimensional commutator on V.

(vi) G is isomorphic to the finitary alternating group $\mathrm{FAlt}(\Omega)$ for some set Ω of size at least 5; the class D corresponds to the class of 3-cycles, or in case $|\Omega|=6$, the class of elements which are products of two disjoint

3-cycles. The space V is the subspace of the space $\mathbb{F}_2\Omega$ generated by all vectors of even weight, or in case $|\Omega|$ is even, the quotient of this space by the all-one vector.

(vii) V carries a G-invariant structure of an $\mathbb{F}_4$-vector space V_4 such that G is isomorphic to $\mathrm{R}(V_4, \Phi)$, where Φ is a subspace of V_4^* annihilating V_4. Here $\mathrm{R}(V_4, \Phi)$ is the subgroup of $\mathrm{GL}(V)$ generated by all its reflections whose axis is a hyperplane of the form $\ker(\phi)$ with $\phi \in \Phi$. The class D is the class of reflections in G.

(viii) V carries a G-invariant structure (V_4, h) of an $\mathbb{F}_4$-vector space V_4 equipped with a nondegenerate hermitian form h such that G is isomorphic to $\mathrm{RU}(V_4, h)$, the subgroup of $\mathrm{GU}(V_4, h)$ generated by all its reflections. The class D is the class of reflections in G.

References

[1] P.J. Cameron, J.I. Hall, Some groups generated by transvection subgroups, *J. Algebra* **140** (1991), 184–209.

[2] A. Chermak, Quadratic pairs without components. *J. Algebra* **258** (2002), no. 2, 442–476.

[3] A. Chermak, Quadratic Pairs, preprint.

[4] A.M. Cohen, H. Cuypers, H. Sterk, Linear groups generated by reflection tori, *Canadian Journal of Mathematics* **56** (1999), 1149-1174.

Base sizes for simple groups and a conjecture of Cameron

Timothy C. Burness

(joint work with Martin Liebeck, Eamonn O'Brien, Aner Shalev, Rob Wilson)

1. Introduction

Let G be a permutation group on a set Ω. A subset of Ω is a *base* for G if its pointwise stabilizer in G is trivial. We write $b(G) = b(G, \Omega)$ for the smallest size of a base for G. Bases have been of interest since the early days of group theory in the nineteenth century. In more recent years, following the seminal work of Sims in the early 1970s, bases have been used extensively in the computational study of finite permutation groups. In this respect, small bases are particularly significant and so it is important to establish accurate bounds on the minimal base size.

Base sizes for finite almost simple primitive groups have been much studied in recent years. A major motivation here comes from a well known conjecture of Cameron and Kantor on so-called *non-standard* permutation groups. Roughly speaking, a finite almost simple primitive permutation group $G \leqslant \mathrm{Sym}(\Omega)$ with socle G_0 is said to be standard if either $G_0 = A_n$ and Ω is an orbit of subsets or partitions of $\{1, \dots, n\}$, or G is a classical group in a subspace action, i.e. Ω is an orbit of subspaces of the natural G-module, or pairs of subspaces of complementary dimension. Non-standard permutation groups are defined accordingly.

In general, it is easy to see that $b(G)$ can be arbitrarily large if G is standard; indeed, the order of such a group is not bounded by a fixed polynomial function of its degree. The Cameron-Kantor Conjecture asserts that this behaviour is a unique feature of standard groups in the sense that there exists an absolute constant c such that $b(G) \leqslant c$ for any non-standard permutation group G. This conjecture was finally settled by Liebeck and Shalev [8] but their proof does not yield an explicit value for c.

2. Cameron's conjecture

In his book *Permutation Groups*, referring to the absolute constant c in the statement of the Cameron-Kantor Conjecture, Cameron writes *"Probably this constant is* 7*, and the extreme case is the Mathieu group* M_{24}*"* (see [5, p.122]). The main result of [3] confirms this conjecture.

Theorem 1. *Let $G \leqslant \mathrm{Sym}(\Omega)$ be a non-standard permutation group. Then $b(G) \leqslant 7$, with equality if and only if G is the Mathieu group M_{24} in its natural action on* 24 *points. Furthermore, the probability that a random* 6*-tuple in Ω is a base for G tends to* 1 *as $|G| \to \infty$.*

Bounds on fixed point ratios play a key role in our proof of Theorem 1. Let G be a permutation group on a finite set Ω and recall that the *fixed point ratio* of $x \in G$, which we denote by $\mathrm{fpr}(x)$, is the proportion of points in Ω which are fixed by x, i.e. $\mathrm{fpr}(x)$ is the probability that a random element of Ω is fixed by x. It is easy to see that if Ω is a transitive G-set then

$$\mathrm{fpr}(x) = \frac{|x^G \cap H|}{|x^G|}, \tag{2.1}$$

where $H = G_\alpha$ is the stabilizer in G of a point $\alpha \in \Omega$. Let $Q(G,c)$ be the probability that a randomly chosen c-tuple of points in Ω is not a base for G, so $b(G) \leqslant c$ if and only if $Q(G,c) < 1$. Of course, a c-tuple in Ω fails to be a base if and only if it is fixed by an element $x \in G$ of prime order; further, the probability that a random c-tuple is fixed by x is at most $\mathrm{fpr}(x)^c$. Now, if G is transitive then fixed point ratios are constant on conjugacy classes (see (2.1)) and thus

$$Q(G,c) \leqslant \sum_{x \in \mathscr{P}} \mathrm{fpr}(x)^c = \sum_{i=1}^{k} |x_i^G| \cdot \mathrm{fpr}(x_i)^c =: \widehat{Q}(G,c), \tag{2.2}$$

where $\mathscr{P}$ is the set of elements of prime order in G, and $x_1, \ldots, x_k$ represent the G-classes of elements in $\mathscr{P}$. Therefore $b(G) \leqslant c$ if $\widehat{Q}(G,c) < 1$, so we can use upper bounds on fixed point ratios to bound the minimal base size.

3. Main results

Let $G \leqslant \mathrm{Sym}(\Omega)$ be a non-standard permutation group with socle G_0. By the Classification of Finite Simple Groups, G_0 is either an alternating group, a group of Lie type (classical or exceptional), or one of 26 sporadic simple groups.

3.1. **Alternating groups.** If G_0 is an alternating group then an easy counting argument due to Cameron and Kantor shows that almost every pair of points in Ω form a base for G. Using similar methods, Guralnick and Saxl have established the following explicit result.

Theorem 3.1 (Guralnick-Saxl, 2004)**.** *Let G be a non-standard permutation group with socle $G_0 = A_n$. Then $b(G) \leqslant 3$, with equality only if $n \leqslant 12$.*

3.2. **Classical groups.** Let G be a non-standard permutation group with socle $G_0 = Cl_n(q)$, a classical group over $\mathbb{F}_q$, with natural module of dimension n.

Theorem 3.2 ([1, Theorem 1])**.** *We have*

$$\mathrm{fpr}(x) < |x^G|^{-\frac{1}{2}+\frac{1}{n}+\iota}$$

for all $x \in G$ of prime order, where either $\iota = 0$, or (G, G_α, ι) is one of a small number of known exceptions.

Set $\zeta_G(t) = \sum_i |x_i^G|^{-t}$, where $t \in \mathbb{R}$ and $x_1, \dots, x_k$ represent the distinct G-classes of elements of prime order in G. Now, if $\iota = 0$ and $n \geqslant 6$ then (2.2) yields

$$Q(G,4) \leqslant \sum_{i=1}^{k} |x_i^G| \cdot \mathrm{fpr}(x_i)^4 < \sum_{i=1}^{k} |x_i^G|^{1+4(-\frac{1}{2}+\frac{1}{n})} \leqslant \zeta_G(1/3)$$

and thus $b(G) \leqslant 4$ since the hypothesis $n \geqslant 6$ implies that $\zeta_G(1/3) < 1$ (see [2, 2.3]). In this way we get the following general result.

Theorem 3.3 ([2, Theorem 1])**.** *Let G be a non-standard classical permutation group. Then either $b(G) \leqslant 4$, or $G = \mathrm{U}_6(2).2$, $G_\alpha = \mathrm{U}_4(3).2^2$ and $b(G) = 5$.*

There are infinitely many examples with $b(G) = 4$. For example, if $G = \Omega_7(q)$ and $G_\alpha = G_2(q)$ (irreducibly embedded) then $b(G) = 4$ for any q.

3.3. **Exceptional groups.** The following theorem is a concise version of the main result of [3] on exceptional groups.

Theorem 3.4 ([3, Theorem 2])**.** *Let G be a faithful primitive almost simple permutation group of exceptional Lie type. Then $b(G) \leqslant 6$.*

Here similar probabilistic methods apply, using (2.2) and the results on fixed point ratios for actions of exceptional groups in [7]. We have better bounds in specific cases. For example, with the aid of some delicate character theoretic calculations we can compute the precise value of $b(G)$ for many parabolic actions. We note that $b(G) = 6$ if $G = E_6(2)$ and $G_\alpha = P_1$ (or P_6), while there are infinitely many examples with $b(G) = 5$, e.g. $G = E_8(q)$ and $G_\alpha = P_8$ for any q. It would be interesting to know if there are only finitely many examples with $b(G) = 6$.

3.4. **Sporadic groups.** Let G be a primitive permutation group with socle a sporadic simple group. In [4] we determine the precise value of $b(G)$, with the exception of two cases involving the Baby Monster. This gives

Theorem 3.5 ([4, Theorem 1]). *We have $b(G) \leqslant 7$, with equality if and only if G is the Mathieu group M_{24} in its natural action on 24 points.*

The proof of this result uses a combination of probabilistic, character theoretic and computational methods. Here the Web-Atlas and the computer package Magma are indispensable tools.

Cameron's Conjecture now follows from Theorems 3.1 and 3.3-3.5.

References

[1] T.C. Burness, *Fixed point ratios in actions of finite classical groups,* I-IV, J. Algebra, to appear.

[2] ——, *On base sizes for actions of finite classical groups*, J. London Math. Soc., to appear.

[3] T.C. Burness, M.W. Liebeck, and A. Shalev, *Base sizes for simple groups and a conjecture of Cameron*, submitted.

[4] T.C. Burness, E.A. O'Brien, and R.A. Wilson, *Base sizes for sporadic simple groups*, in preparation.

[5] P.J. Cameron, *Permutation Groups*, London Math. Soc. Student Texts, vol. 45, Cambridge University Press, 1999.

[6] J.P. James, *Partition actions of symmetric groups and regular bipartite graphs*, Bull. London Math. Soc. **38** (2006), 224–232.

[7] R. Lawther, M.W. Liebeck, and G.M. Seitz, *Fixed point ratios in actions of finite exceptional groups of Lie type*, Pacific J. Math. **205** (2002), 393–464.

[8] M.W. Liebeck and A. Shalev, *Simple groups, permutation groups, and probability*, J. Amer. Math. Soc. **12** (1999), 497–520.

Simplicity of some infinite automorphism groups

Dugald Macpherson
(joint work with Katrin Tent)

This talk describes a proof of the simplicity of a reasonably rich class of automorphism groups.

The framework is model-theoretic. Let L be a finite relational first-order language. A countably infinite L-structure M is *homogeneous* if any isomorphism between finite (induced) substructures of M extends to an automorphism of M. Given such (homogeneous) M, let $\mathcal{A}(M)$, the *age* of M, be the collection of finite L-structures which embed in M. It is easily checked that $\mathcal{A}(M)$ is closed under isomorphism and substructure, has the joint embedding property, and also has the *amalgamation property*: namely, if $A, B_1, B_2 \in \mathcal{A}(M)$ and $f_i : A \to B_i$ are embeddings, there is $C \in \mathcal{A}(M)$ and $g_i : B_i \to C$ (for $i = 1, 2$) such that $g_1 \circ f_1 = g_2 \circ f_2$. We say that a class of finite L-structures with these four properties is an *amalgamation class*. R. Fraïssé [1] proved a converse: if $\mathcal{C}$ is an amalgamation class with arbitrarily large finite members, then there is a unique countably infinite homogeneous L-structure M with $\mathcal{A}(M) = \mathcal{C}$. We call M the *Fraïssé limit* of $\mathcal{C}$. In the particular case when $g_1(B_1) \cap g_2(B_2) = g_1(f_1(A))$ and any tuple of C satisfying a relation of L lies in $g_1(B_1)$ or in $g_2(B_2)$, we say that C is a *free amalgam*. We say that M is a *free homogeneous structure* if it is homogeneous and the amalgamation for its age can always be done freely.

The main theorem is the following.

Theorem 1. *Let M be a countably infinite free homogeneous L-structure such that $G := \mathrm{Aut}(M)$ is transitive but not equal to $\mathrm{Sym}(M)$. Then G is a simple group.*

As a special case of this, Truss [4] proved that the automorphism group of the random graph (whose age is the collection of all finite graphs) is simple. In unpublished work, M. Rubin extended this to a broader class of homogeneous L-structures with L binary, and with a hypothesis rather similar to free amalgamation. Much more recently, S. Lovell [3] combined some of these ideas, and was able to prove, for example, that for $k \geq 2$ the automorphism group of the universal homogeneous k-hypergraph is simple. In one respect our proof gives less information than these, as we do not show that there is some fixed natural number c such that if $g, h \in G \setminus \{1\}$ then h is a product of at most c conjugates of g and g^{-1}. However, our proof seems relatively short, notationally light, and flexible: it ought for example to yield simplicity of the automorphism groups of certain Hrushovski constructions, and perhaps of the automorphism groups of certain generalised polygons, constructed by Tent – groups which admit BN-pairs.

Our proof mimics that of Lascar [2], and uses the Polish group structure on G, induced from the topology of pointwise convergence on $\mathrm{Sym}(M)$. Basic open subgroups of G are pointwise stabilisers of finite sets. Elementary arguments yield the following, under the assumptions of the theorem.

(i) G acts primitively on M.

(ii) G has no proper non-trivial open normal subgroups.

(iii) If $g \in G \setminus \{1\}$, then there is $h \in G$ such that the commutator $[g, h]$ has no 1-cycles or 2-cycles.

Let H be a non-trivial normal subgroup of G, and $g \in H \setminus \{1\}$. We may suppose, by (iii), that g has no 1-cycles or 2-cycles. Define $\alpha : G^4 \to G$ by $\alpha(u, v, w, z) = g^u g^v g^w g^z$, and put $E := \mathrm{Im}(\alpha)$. Easily, the group $\langle E \rangle$ has the Baire Property, so by a well-known fact about Polish groups, $\langle E \rangle$ is meagre or open. If E is open, then $\langle E \rangle = G = H$ by (ii), so it remains to show that E is not meagre. For this, the following lemma suffices.

Lemma 1. *Let U_1, U_2, U_3, U_4 be non-empty open subsets of G. Then there is a non-empty open V such that $\alpha(U_1 \times U_2 \times U_3 \times U_4)$ is dense in V.*

References

[1] R. Fraïssé, *Sur certains relations qui généralisent l'ordre des nombres rationnels*, C.R. Acad. Sci. Paris **237**, 540–542.

[2] D. Lascar, *Les automorphismes d'un ensemble fortement minimal*, J. Symb. Logic **57** (1992), 238–251.

[3] S. Lovell, *Automorphism groups of homogeneous structures*, PhD thesis, University of Leeds, 2007.

[4] J.K. Truss, *The group of the countable universal graph*, Math. Proc. Cam. Phil. Soc. **105** (1989), 223–236.

Finite simple groups and expander graphs

Martin Kassabov
(joint work with A. Lubotzky and N. Nikolov)

Expanders are highly connected finite graphs which play a fundamental role in theoretical computer science. Informally, a graph is an expander if it cannot be separated into two large pieces by removing a small number of vertices and the adjoining edges.

Definition. A finite graph Γ is called an ϵ-*expander*, if for any set of vertices I such that $|I| \leqslant |\Gamma|/2$ we have $|\partial I| \geq \epsilon|I|$, where ∂I is the set of vertices in $\Gamma \setminus I$ which are connected to some vertex in I. The maximal ϵ with this property is called the *expanding constant* for the graph Γ.

A family of graphs is called an *expander family* if they are ϵ-expanders for some positive ϵ and their size goes to infinity. Many applications impose an additional requirement that the number of edges does not grow too fast because the edges are associated with the 'cost' of the graph.

The existence of families of expander graphs follows from a standard counting argument showing that a randomly chosen graph is a good expander. Unfortunately this argument does not allow for the explicit construction of expanders, which is required for many applications.

A big class of finite graphs with applications in discrete mathematics are constructed using finite groups: the elements of a finite group G form the set of vertices of the Cayley graph $\mathcal{C}(G;S)$ and two elements g and h are connected by an edge if gh^{-1} or hg^{-1} is in some fixed generating set S. There is great practical interest in developing methods for estimating the expanding constant of Cayley graphs and constructing families of groups G_i together with generating sets S_i such that $\mathcal{C}(G_i;S_i)$ is a family of expanders.

The expanding constant of a graph is closely related to other important graph invariants like the Cheeger constant, the spectrum of the adjacency matrix and the spectral gap of the discrete Lapacian. Relying on these connections Margulis constructed the first explicit family of expander graphs using Kazhdan property T for $\mathrm{SL}_3(\mathbb{Z})$, which comes from the representation theory of Lie groups. It is possible to estimate the expanding constants of the resulting graphs if a quantitative version of property T is known, e.g. if there are bounds for the Kazhdan constants.

Computing Kazhdan constants requires detailed knowledge of all unitary representations of the group. The exact value of the Kazhdan constant is known only in a few special cases.

In recent years there have been several results using group structure to obtain bounds for the Kazhdan constants. These techniques not only produce estimates of the Kazhdan constants but also provide direct proofs that some families of Cayley graphs are expanders.

Problem. Let G_i be an infinite family of finite groups. Is it possible to make their Cayley graphs expanders using suitably chosen generating sets of bounded size?

The answer is known only in a few special cases: if the groups in the family are quotients of a finitely generated infinite group with property Tau (or its weaker versions) then the answer is YES. Lubotzky and Weiss proved that if all groups in the family are solvable of bounded derived class then the answer is NO, and this is practically the only case where a negative answer is known.

In order to answer this problem one needs to estimate the Kazhdan constants of G_i with respect to various generating sets. The following conjecture from [1] is a special case for the family of all non-abelian finite simple groups.

Conjecture [Babai-Kantor-Lubotzky]. There exist constants $L > 0$ and $\epsilon > 0$ such that any non-abelian finite simple group G has a generating set F such that $|F| \leqslant L$ and the Cayley graphs $\mathcal{C}(G; F)$ form a family of expanders.

There are several results supporting this conjecture – it is known that any non-abelian finite simple group admits a 4-element generating set, such that the diameter of the corresponding Cayley graph is logarithmic in the size of the group. It is also known that several families of finite simple groups admit expanding generating sets.

Our main result confirms the Babai-Kantor-Lubotzky conjecture except in the case of Suzuki groups. The main method used to obtain this result relies on the relationships between the Kazhdan constants of a given group with respect to different generating sets and some easy estimates of relative Kazhdan constants. In the case of groups of Lie type our construction heavily relies on the fact that any finite simple group of Lie type can be decomposed as a product of 27 abelian groups. Unfortunately a similar result does not hold for the the family of the alternating groups. In this case we use several embeddings of groups of Lie type in large alternating groups and apply estimates for the characters of the symmetric groups and some probabilistic techniques.

References

[1] L. Babai, W. M. Kantor, A. Lubotzky, *Small-diameter Cayley graphs for finite simple groups*, European J. Combin. **10** (1989), no. 6, 507–522.

Intervals in subgroup lattices of finite groups

Michael Aschbacher

Let G be a finite group and $H \leqslant G$. Write $\mathcal{O}_G(H)$ for the lattice of overgroups of H in G. We show that suitable constraints on the lattice $\mathcal{O}_G(H)$ impose strong restrictions on the structure of G, and then use this result to investigate two problems.

The functional analyst Watatani showed that among the lattices with six elements, all but possibly two are lattices of intermediate subfactors in some von Neumann algebra. In response to questions raised by functional analysts, we show that for each of the two Watatani lattices Λ, there exists a finite group G and a subgroup H of G such that $\mathcal{O}_G(H) \cong \Lambda$. Hence by a so-called “cross product construction”, the two lattices *are* lattices of intermediate subfactors.

The following question (suggested by a theorem of Palfy and Pudlak) has been open for at least 25 years:

Question. Is each nonempty finite lattice isomorphic to a lattice $\mathcal{O}_G(H)$ for some finite group G and subgroup H?

Define a $\Delta(3)D$-lattice to be a disconnected lattice whose connected components are isomorphic to the lattice of subsets of a 3-set. The author and John Shareshian have begun a program to show the Question has a negative answer, by showing:

(*) No $\Delta(3)D$-lattice is of the form $\mathcal{O}_G(H)$.

As a first step in that program, we show that if (*) fails, then there exists an almost simple group G such that either:

(1) There exists $H \leqslant G$ such that $\mathcal{O}_G(H)$ is a $\Delta(3)D$-lattice, or

(2) there exists a lower signalizer lattice Δ generating G, such that Δ is a $\Delta(3)D$-lattice.

The lattice Δ is defined by a pair of subgroups N, I of G such that $I \trianglelefteq N$, N/I is almost simple, and $\Delta = \{\infty\} \cup \mathcal{W}$, where

$$\mathcal{W} = \{W \leqslant F^*(G)I : W \text{ is } N\text{-invariant and } W \cap N = I\},$$

with $\mathcal{W}$ partially ordered by inclusion.

To complete the program it remains to show that no almost simple group satisfies (1) or (2).

Edge-primitive graphs

Michael Giudici
(joint work with Cai Heng Li)

Let Γ be a finite graph and $G \leqslant \mathrm{Aut}(\Gamma)$. We say that Γ is *G-edge-primitive* if G acts primitively on the set of edges of Γ. Many well known graphs are edge-primitive, for example, the Heawood graph, the Hoffman-Singleton graph and the Higman-Sims graph, as well as many of the rank three graphs of sporadic simple groups. Weiss [2] showed that the only edge-primitive graphs of valency three are the complete bipartite graph $K_{3,3}$, the Heawood graph, the Biggs-Smith graph and the Tutte-Coxeter graph.

Let $\mathcal{B}$ be a system of imprimitivity of G on the set $V\Gamma$ of vertices of Γ. We can define the *quotient graph* $\Gamma_{\mathcal{B}}$ of Γ to be the graph with vertex set $\mathcal{B}$ and two blocks $B_1, B_2 \in \mathcal{B}$ are adjacent if and only if there exist vertices $v \in B_1$ and $w \in B_2$ such that v and w are adjacent in Γ. If for each edge $\{B, C\}$ of $\Gamma_{\mathcal{B}}$ the subgraph of Γ induced on $B \cup C$ is a matching we say that Γ is a *cover* of $\Gamma_{\mathcal{B}}$, while if for each edge $\{B, C\}$ there is a unique edge in the subgraph induced on $B \cup C$ we say that Γ is a *spread* of $\Gamma_{\mathcal{B}}$.

We say that a transitive permutation group G is *biprimitive* if it is not primitive and all systems of imprimitivity have precisely two blocks. If $|\Omega| > 4$ then such a system is unique and G has an index two subgroup G^+ which acts primitively on each of its two orbits. Note that if a group G acts biprimitively on a graph Γ then Γ is bipartite with the bipartition being a system of imprimitivity. We say that Γ is G-locally imprimitive if for each vertex v, the vertex stabiliser G_v acts imprimitively on the set of neighbours of v.

We have the following result from [1].

Theorem 1. *Let Γ be a connected G-edge-primitive graph. Then one of the following holds:*

(i) Γ *is a star.*
(ii) G *is vertex-primitive.*
(iii) G *is vertex-biprimitive.*
(iv) Γ *is a spread of a G-edge-primitive, G-locally imprimitive graph.*

Conversely, any G-edge-primitive, G-locally imprimitive graph Σ is a quotient of a larger G-edge-primitive graph Γ such that $G^{E\Gamma} = G^{E\Sigma}$.

The star case in Theorem 1 is the only instance where an edge-primitive graph is not vertex-transitive.

Theorem 1 leads us to study edge-primitive graphs which are either vertex-primitive or vertex-biprimitive. In the vertex-primitive case G has a primitive action on both vertices and edges, while in the vertex-biprimitive case G has a primitive action on edges and an index two subgroup G^+ which acts primitively on each of its vertex orbits. This allows an analysis of the possible O'Nan-Scott types for the primitive actions of G and G^+. Such an investigation was undertaken in [1] where it was seen that the important case to study is the case where G is an almost simple group acting primitively on edges and either primitively or biprimitively on vertices. An initial investigation of this case was undertaken with a complete determination of all G-edge-primitive graphs where $\mathrm{soc}(G) = \mathrm{PSL}\,(2,q)$. Apart from the complete graph, there are two infinite families and 8 sporadic examples.

References

[1] M. Giudici and C. H. Li, *On finite edge-primitive graphs*, submitted. Preprint available online at

http://www.maths.uwa.edu.au/~giudici/research.

[2] R. M. Weiss, *Kantenprimitive Graphen vom Grad drei*, J. Combin. Theory Ser. B **15** (1973) 269–288.

Progress report on the classification of imprimitive finite distance-transitive graphs

Jonathan I. Hall

(joint work with M.R. Alfuraidan)

A distance-transitive graph G is one upon which the automorphism group acts transitively on ordered pairs of vertices at every fixed distance. Only connected graphs need to be considered.

The classification of finite distance-transitive graphs naturally breaks into two parts—primitive and imprimitive. The main part of the problem is the classification of all finite distance-transitive graphs with primitive automorphism group, and it appears [3] that this classification is nearly finished.

In the imprimitive case Derek Smith [11] showed that the possibilities for nontrivial blocks of imprimitivity are severely limited and that a given imprimitive distance-transitive graph can in a sense be reduced to a primitive distance-transitive graph.

The distance-transitive graph G of diameter d is *antipodal* if the relation of being at distance d is a transitive relation on the vertices of G. We write AG for the quotient graph induced on the antipodal classes of an antipodal graph G. The graph AG is itself distance-transitive.

If the distance-transitive graph G is bipartite, then a *halved graph* BG is one of the connected components under the adjacency relation of being at distance 2 in G. The two halved graphs BG are isomorphic distance-transitive graphs.

In [1] a version of Smith's Theorem was proven. (The parameter μ is the number of common neighbors of two vertices at distance two.)

Theorem. *Let G be a finite connected distance-transitive graph of diameter d and valency k. Set $k' = k(k-1)/\mu$. Then one of:*

(1) G is primitive of diameter $d \geq 2$ and valency $k \geq 3$;

(2) $k = 2$, $d = \lfloor n/2 \rfloor$, and G is a cycle C_n for some $n \geq 3$;

(3) $d \leq 1$, and G is a complete graph K_{k+1};

(4) $d = 2$, and G is a complete multipartite graph $K_{r,\dots,r}$ with $1 + \frac{k}{r}$ parts of size $r \geq 2$;

(5) *$d = 3$, and G is the bipartite incidence graph of a nontrivial symmetric design with block size $k \geq 3$ and index μ;*

(6) *$d = 3$, and G is an antipodal cover of K_{k+1} with $k \geq 3$;*

(7) *$d = 4$; G is antipodal and bipartite; $\mathrm{A}G$ is $K_{k,k}$ with $k \geq 3$, and $\mathrm{B}G$ is complete multipartite;*

(8) *$d = 6$; G is antipodal and bipartite; $\mathrm{A}G$ is bipartite of diameter 3, and $\mathrm{B}G$ is antipodal of diameter 3; the graph $\mathrm{BA}G = \mathrm{AB}G$ is $K_{k'+1}$, for $k' \geq k \geq 3$;*

(9) *$d \geq 4$; G is antipodal but not bipartite, and $\mathrm{A}G$ is primitive of diameter $c = \lfloor d/2 \rfloor \geq 2$ and valency $k \geq 3$;*

(10) *$d \geq 4$; G is bipartite but not antipodal, and $\mathrm{B}G$ is primitive of diameter $c = \lfloor d/2 \rfloor \geq 2$ and valency $k' \geq k \geq 3$;*

(11) *odd $d = 2c + 1 \geq 5$; G is antipodal and bipartite; all antipodal classes have size 2, and $\mathrm{A}G$ is primitive of diameter $c \geq 2$ and valency $k \geq 3$; $\mathrm{B}G$ is primitive of diameter $c \geq 2$ and valency $k' \geq k \geq 3$;*

(12) *even $d = 2e \geq 8$; G is antipodal and bipartite; $\mathrm{A}G$ is bipartite of diameter e, and $\mathrm{B}G$ is antipodal of diameter e; the graph $\mathrm{BA}G = \mathrm{AB}G$ is primitive of diameter $c = \lfloor e/2 \rfloor \geq 2$ and valency $k' \geq k \geq 3$.*

As already mentioned, it appears [3] that in the primitive case (1) the classification is nearly finished.

Under the seven exceptional cases (2-8) all distance-transitive graphs are known. The specific graphs of (2-4) are all distance-transitive. The classification of distance-transitive antipodal covers of complete graphs, as in (6), and of complete bipartite graphs, as in (7), has been completely settled by, respectively, Godsil, Liebler, and Praeger in [6] and Ivanov, Liebler, Penttila, and Praeger in [9]. The bipartite, diameter 3 graphs of (5) are exactly the incidence graphs of nontrivial symmetric designs. As such, those that are distance-transitive were classified by Kantor [10]. It is shown in [1, Theorem 3.3] that the 6-cube $H(6, 2)$ is the unique distance-transitive graph coming under (8).

This leaves the four generic imprimitive cases (9-12). We proceed under the assumption that the list of known primitive graphs as in (1) is complete. We then need only consider imprimitive distance-transitive graphs G for which one of $\mathrm{A}B$, $\mathrm{B}G$, or $\mathrm{AB}G = \mathrm{BA}G$ is a known primitive distance-transitive graph of valency at least three and diameter c at least two.

Many of the cases were handled by Van Bon and Brouwer [4] and Hemmeter [7, 8]. The completed classification under the additional assumption that the core diameter c is at least three is given in [2]. There are no surprises—the only associated imprimitive graphs are ones already known and in the literature; see [5].

The remaining case $c = 2$ is under study.

References

[1] M.R. Alfuraidan and J.I. Hall, Smith's Theorem and a characterization of the 6-cube as distance-transitive graph, J. Algebraic Combin. **24** (2006), 195–207.

[2] M.R. Alfuraidan and J.I. Hall, Imprimitive distance-transitive graphs with primitive core of diameter at least three, submitted.

[3] J. van Bon, Finite primitive distance-transitive graphs, European J. Combin. **28** (2007), 517–532.

[4] J.T.M. van Bon and A.E. Brouwer, The distance-regular antipodal covers of classical distance-regular graphs, in: Colloq. Math. Soc. Janos Bolyai, Proc. Eger 1987, 1988, 141–166.

[5] A.E. Brouwer, A.M. Cohen, and A. Neumaier, "Distance-regular Graphs," Springer, Berlin, 1989.

[6] C.D. Godsil, R.A. Liebler, and C.E. Praeger, Antipodal distance transitive covers of complete graphs, Europ. J. Combin. **19** (1998), 455–478.

[7] J. Hemmeter, Halved graphs, Johnson and Hamming graphs, Utilitas Math. **25** (1984), 115–118.

[8] J. Hemmeter, Distance-regular graphs and halved graphs, Europ. J. Combin. **7** (1986), 119–129.

[9] A.A. Ivanov, R.A. Liebler, T. Penttila, C.E. Praeger, Antipodal distance-transitive covers of complete bipartite graphs, European J. Combin. **18** (1997), 11–33.

[10] W.M. Kantor, Classification of 2-transitive symmetric designs, Graphs Combin. **1** (1985), 165–166.

[11] D.H. Smith, Primitive and imprimitive graphs, Quart. J. Math. Oxford (2) **22** (1971), 551–557.

Unipotent and nilpotent classes in simple algebraic groups and Lie algebras

Gary M. Seitz

(joint work with Martin W. Liebeck)

Let G be a simple algebraic group over an algebraically closed field K of arbitary characteristic p. Our project is aimed at a new approach to understanding the conjugacy classes and centralizers of unipotent elements in G and nilpotent elements of $L(G)$, along with corresponding results for the finite groups of Lie type.

While there is a considerable literature on unipotent classes in algebraic groups, it is scattered across many papers using different methods and notations. Moreover, when p is a bad prime for G there are very few results giving the precise centralizers of nilpotent elements, even for the classical groups. Our goal is to cover both unipotent and nilpotent elements in all characteristics.

The approach we use is to first obtain complete results for nilpotent classes and centralizers and to then use this information to obtain corresponding results for unipotent classes. At the time of writing, we have complete results for $p \neq 2$ and the analysis for $p = 2$ is in progress.

The following is one of the results we obtain. To state it we require some notation. For each nilpotent element $e \in L(G)$, we produce a 1-dimensional torus T such that $T(c)e = c^2e$ for $0 \neq c \in K$. There is a fundamental system of roots for which T acts by a non-negative weight on each of the corresponding root elements of $L(G)$. In this way T determines a labelling of the Dynkin diagram of G by non-negative integers. The torus T also determines a parabolic subgroup $P = QK$ of G, where $K = C_G(T)$ is the Levi factor (corresponding to the zero labels) and the unipotent radical Q is the product of all root subgroups for which the root affords a positive weight of T. Let $Q_{\geq 2}$ denote the product of all root groups for which the T-weight is at least 2. Our choice then gives $e \in L(Q_{\geq 2})$.

Theorem. *Let G be a simple algebraic group over an algebraically closed field K of characteristic p. Assume $p \neq 2$ if G is not of type A_n. Then there is a bijective correspondence between the unipotent classes of G and the nilpotent classes of $L(G)$, such that if $u \in G$ and $e \in L(G)$ are corresponding representatives, the following hold.*

(i) *$C_G(e) = R_u(C_G(e))(C_G(T) \cap C_G(e))$, a semidirect product, where T is as above.*

(ii) *$\dim R_u(C_G(u)) = \dim R_u(C_G(e))$.*

(iii) *$C_G(u)/R_u(C_G(u)) \cong C_G(e)/R_u(C_G(e))$ or $C_G(e)/R_u(C_G(e)) \times Z_p$. The latter case is only possible if p is a bad prime, and when it does occur, $u \notin R_u(C_G(u))$.*

(iv) *Let $P = QK$ be the parabolic subgroup of G determined as above. Then $C_G(e) \leq P$. With the exception of one pair of classes in E_8 and one pair in G_2, both with $p = 3$, e^P is open dense in $L(Q_{\geq 2})$ and $e^Q = e + L(Q)_{>2}$. Moreover, u can be chosen such that $u \in Q$, $C_G(u) \leq P$, and except for the pairs above, u^P is open dense in $Q_{\geq 2}$ and $u^Q = uQ_{>2}$.*

The exceptional pairs mentioned in (iv) arise from one class in each of E_8 and G_2, both for $p = 3$, where the centralizer has larger dimension than usual. In each case there exists an exceptional, but closely related class. In addition to the above result we also obtain precise information on centralizers, some of which is new even in good characteristic or 0. For example, we obtain information about the embedding of the reductive part of centralizers that yields an understanding of the component groups.

Our analysis proceeds as follows. As mentioned above we start with nilpotent elements. If e is a nilpotent element in $L(G)$, let T_0 be a (possibly trivial) maximal torus of $C_G(e)$. Then $C_G(T_0) = L = L'T_0$ is a Levi subgroup. Moreover e is a *distinguished* nilpotent element of $L(L')$, meaning that $C_{L'}(e)^0$ is a unipotent group. In good characteristic, the Bala-Carter theory shows that such elements arise from certain parabolic subgroups of L', called *distinguished* parabolic subgroups. But in bad characteristic, the existence of such elements is not easy. Our first major goal is to produce an explicit distinguished nilpotent element of $L(L')$ corresponding to each distinguished parabolic of L'. In doing so we also produce the 1-dimensional torus T as in (i). The factorization in (i) is a key result, one that holds quite generally. The centralizer of e in L' is determined. The analysis of distinguished nilpotent elements is quite interesting and eventually leads to a clear understanding of how and why the Z_p factor in (iii) arises.

The next phase of the program is to consider the restriction of $L(G)$ to L', in order to determine the precise centralizer of e in G, using (i) and aspects of the representation theory of L' on $L(G)$. This analysis leads to the exceptional classes mentioned above which exist only for $p = 3$. At this point we must show our list of class representatives is complete. The main case is the exceptional groups and one way to proceed in positive characteristic is to use Lang's theorem, work at the level of finite groups of Lie type, and count to see that we have the correct number. This is a straightforward process. Proceeding in this way the analysis yields a direct proof of the finiteness of the number of nilpotent classes.

We next proceed to the analysis of unipotent classes which is now relatively simple. Each of the nilpotent class representatives e produced above has an explicit form as a sum of root elements with coefficients ±1. There is a corresponding unipotent element, say u, which is the product of the root group elements with the same coefficient, in some fixed order. We establish some general results which relate the centralizers of these nilpotent and unipotent elements. In particular, the density information in (iv) for e, yields corresponding information for u. To show our list of unipotent elements is complete, one can argue that the count for unipotents follows immediately from that of nilpotents.

The analysis for $p = 2$ is now under way. Here the classical groups are a key issue. Our starting point is a nice paper of Hesselink describing conjugacy classes and dimensions of centralizers. We are reorganizing this material so that it fits with our starting point of finding distinguished nilpotent elements in Levi subgroups. From here we find $C_G(T) \cap C_G(e)$, which turns out to be very nice. The next step is to analyse centralizers of corresponding unipotent elements, which is more complicated. While there is no longer a bijection between unipotent and nilpotent classes, we do produce an explicit injection from unipotent classes to nilpotent classes. Finally, for exceptional groups with $p = 2$, we plan to proceed in similar fashion to the analysis for other characteristics.

Permutation groups of finite Morley rank

Alexandre V. Borovik
(joint work with Gregory Cherlin)

Groups of finite Morley rank made their first appearance in model theory as *binding groups*, which are the key ingredient in Zilber's ladder theorem and in Poizat's explanation of the Picard-Vessiot theory. These are not just groups, but in fact permutation groups acting on important definable sets. When they are finite, they are connected with the model theoretic notion of algebraic closure. But the more interesting ones tend to be infinite, and connected.

Many problems in finite permutation group theory became tractable only after the classification of the finite simple groups. The theory of permutation groups of finite Morley rank is not very highly developed, and while we do not have anything like a full classification of the simple groups of finite Morley rank in hand, as a result of recent progress [1, 2] we do have some useful classification results as well as some useful structural information that can be obtained without going through an explicit classification. So it seems like a good time to review the situation in the theory of permutation groups of finite Morley rank and to lay out some natural problems and their possible connections with the body of research that has grown up around the classification effort.

The study of transitive permutation groups is equivalent to the study of pairs of groups (G, H) with H a subgroup of G, and accordingly one can read much of general group theory as permutation group theory, and vice versa, and, indeed, a lot of what goes on in work on classification makes a good deal of sense as permutation group theory—including even the final identification of a group as a Chevalley group, which can go via Tits' theory of buildings, or in other words by recognition of the natural permutation representations of such groups.

The most important class of permutation groups consists of the *definably primitive* permutation groups, and in finite group theory one has the O'Nan-Scott-Aschbacher classification of these groups into various families, determined mainly by the structure of the socle and the way it meets a point stabilizer. This theorem has been adapted to the context of finite Morley rank by Macpherson and Pillay [6], and is the one really general piece of work in the area to date. Also noteworthy is the classification by Hrushovski of groups acting faithfully and definably on strongly minimal sets [7, Th. 3.27], and the study by Gropp [4] of the rank two case.

It turns out that basic notions of permutation group theory such as primitivity and multiple transitivity have more than one useful analog in the context of groups of finite Morley rank, for two reasons: (a) we are interested particularly in connected groups (and, by implication, sets of Morley degree 1); (b) we are interested in generic behavior. Of course we also impose definability constraints. So we have definable primitivity and some analogs involving connectivity, and we have generic n-transitivity, which is far more common than ordinary n-transitivity. Indeed, sharp 4-transitivity cannot occur on an infinite set [5], while $\mathrm{AGL}(V)$ acts generically sharply $(n+1)$-transitively on V if V has dimension n, with $\mathrm{PGL}(V)$ generically sharply $(n+1)$-transitive on projective space, with similar, though less extreme, statements for other classical groups acting naturally.

Our principal result is the following

Main Theorem. *The Morley rank of a definably primitive permutation group of finite Morley rank is bounded by a function of the rank of the set on which it acts.*

Surprisingly, this result was previously unknown even for rational actions of algebraic groups. Easy examples show that the definable primitivity assumption cannot be omitted from the formulation of the theorem.

Our proof involves establishing bounds for the possible degree of generic multiple transitivity of permutation groups of finite Morley rank. We are not very precise in our estimates, but one may expect that very good bounds should hold in this part of the process, as generically highly transitive groups should be rare outside of known examples. This is a problem which makes sense and is interesting for groups of finite Morley rank in general, for simple algebraic groups acting definably, and even for simple algebraic groups acting algebraically. In the latter case it has been solved in characteristic 0 by Popov [8], using some results of Kimura et al. on rational representations with an open orbit.

The following result, controlling what one might reasonably call "Lie rank", plays an important role in our "soft" analysis and could also be of use in more concrete approaches.

Lemma. *Let (G, Ω) be a definably primitive permutation group of finite Morley rank, T a definable divisible abelian subgroup of G, T_0 its torsion subgroup, and $O(T)$ the largest definable torsion free subgroup of T. Then* $\mathrm{rk}(T/O(T)) \leq \mathrm{rk}(\Omega)$.

An approach to the study of permutation groups of finite Morley rank outlined in this talk became possible only because of the recently completed classification of simple groups of finite Morley rank and even type [1] and structural results for groups of finite Morley rank with finite Sylow 2-subgroups [3].

The full proof of the results in this talk will appear in [2].

References

[1] T. Altınel, A. Borovik, and G. Cherlin, **Simple Groups of Finite Morley Rank**. Amer. Math. Soc., 554 + xvi pp., to appear in 2008.

[2] A. V. Borovik and G. Cherlin, *Permutation groups of finite Morley rank*, to appear in the Proceedings of Sir Isaak Newton Institute.

[3] A. V. Borovik, J. Burdges and G. Cherlin, *Involutions in in groups of finite Morley rank of degenerate type*, Selecta Math. **13** no. 1, 1–22. DOI 10.1007/s00029-007-0030-z.

[4] U. Gropp, *There is no sharp transitivity on q^6 when q is a type of Morley rank* 2, J. Symbolic Logic 57 (1992) 1198–1212.

[5] M. Hall, Jr., *On a theorem of Jordan*, Pacific J. Mathematics 4 (1954) 219–226.

[6] H. D. Macpherson and A. Pillay, *Primitive permutation groups of finite Morley rank*, Proc. London Math. Soc. 70 (1995) 481–504.

[7] B. Poizat, **Groupes Stables**. Nur Al-Mantiq Wal-Ma'rifah, Villeurbanne, France, 1987; English translation 2001, AMS.

[8] V. Popov, Generically multiply transitive algebraic group actions. Preprint, 2005.

On semiprimitive permutation groups

Attila Maroti

A permutation group is called *semiregular* if all point-stabilizers are trivial. A permutation group is called *regular* if it is semiregular and transitive. We say that a transitive but not regular permutation group G is *semiprimitive* if all normal subgroups of G are transitive or semiregular.

Non-regular primitive, quasiprimitive, innately transitive groups are semiprimitive. Hence it may be interesting to classify semiprimitive groups. Another motivation for such a classification comes from universal algebra.

Aron Bereczky and I mainly worked on classifying solvable semiprimitive groups. We proved that a solvable semiprimitive group G contains a unique regular normal subgroup K and this subgroup has the property that any normal subgroup of G contains K or is contained in K. We called such a group K the kernel of the group G.

This nomination comes from the fact that Frobenius groups are semiprimitive. However, whereas the kernel of a Frobenius group is necessarily nilpotent by a theorem of Thompson, the kernel of a solvable semiprimitive group need not be nilpotent. There are examples of Coxeter groups with non-nilpotent kernels.

The strongest theorem of our paper is a classification of solvable semiprimitive groups of degrees products of at most three primes.

The Ore conjecture

Martin W. Liebeck
(joint work with E.A. O'Brien and A. Shalev)

The Ore conjecture states that every element of every finite non-abelian simple group is a commutator. It was proved for the alternating groups by Ore himself in [8], and for $PSL_n(q)$ in a series of papers [10, 11, 12] by R.C. Thompson. Later progress was achieved by various authors, notably Gow, who showed in [4] that the Ore conjecture holds for the symplectic groups $PSp_{2n}(q)$ if $q \equiv 1 \bmod 4$, and in [5] that every semisimple element of a finite simple group of Lie type is a commutator. The sporadic groups were handled in [7]. Bonten [1] proved the conjecture for exceptional groups of Lie type apart from the types E_6, ${}^2E_6$, E_7 and E_8. Finally, Ellers and Gordeev [2] have shown that Ore's conjecture holds for groups of Lie type over $GF(q)$, provided q is not too small ($q \geq 8$ suffices, although for several families their bound is better than this).

In this report we announce a proof of Ore's conjecture for some additional families of simple groups – namely, all symplectic groups and all exceptional groups of Lie type. Hence to prove the conjecture in full, it remains only to handle unitary and orthogonal groups over small fields.

Theorem 1. *Every element of the symplectic group $Sp_{2m}(q)$ is a commutator, excluding $Sp_2(2), Sp_2(3)$ and $Sp_4(2)$.*

Theorem 2. *Let G be one of the simple groups $E_6^\epsilon(q)$, ${}^2E_6(q)$, $E_7(q)$ or $E_8(q)$. Then every element of G is a commutator.*

These results are proved in [6].

Notice that Theorem 1 gives a little more than the Ore conjecture in the symplectic case, since it deals not just with the simple groups $PSp_{2m}(q)$, but also with the central extensions $Sp_{2m}(q)$. Of course the excluded groups $Sp_2(2), Sp_2(3)$ and $Sp_4(2)$ are genuine exceptions, since they are not perfect.

The strategy of the proof combines three main ingredients: character theory, induction on the dimension, and certain computer calculations.

The connection with character theory is based on the classical result of Frobenius that an element g of a finite group G is a commutator if and only if

$$\sum_{\chi \in \mathrm{Irr}(G)} \chi(g)/\chi(1) \neq 0,$$

where the sum is over the set $\mathrm{Irr}(G)$ of irreducible characters of G. The Deligne-Lusztig theory of irreducible characters of groups of Lie type can be used to derive information on character values and degrees. Roughly speaking, we show that if g is an element with a small centralizer, then the numbers $|\chi(g)|/\chi(1)$ are small for $\chi \neq 1$, and the main contribution to the sum $\sum_{\chi \in \mathrm{Irr}(G)} \chi(g)/\chi(1)$ comes from the trivial character $\chi = 1$. This enables us to deduce that this sum is positive, so elements with small centralizer are commutators.

For elements whose centralizers are not small, our strategy is to reduce to groups of Lie type of lower dimension and use induction. In our proof for symplectic groups, this is usually possible since such elements have a Jordan decomposition into several Jordan blocks, and hence lie in a corresponding product of smaller symplectic groups. However, various technical difficulties have to be overcome to make this idea work. For instance, some blocks may lie in a tiny symplectic group which is not perfect, such as $Sp_2(2)$, $Sp_2(3)$ or $Sp_4(2)$. For exceptional groups, again the aim is to show that elements with reasonably large centralizer lie in suitable semisimple subsystem subgroups so that induction can be applied. This is achieved using a large amount of technical information on centralizers in these groups.

Finally, since the proofs are inductive, we need to establish various base cases. This is done largely using computational methods.

We note that some very recent probabilistic results provide further evidence towards the validity of Ore's conjecture. In [9] it is shown that, if $Com(G)$ is the set of commutators in the finite simple group G, then $|Com(G)|/|G| \to 1$ as $|G| \to \infty$, and so a random element is very likely to be a commutator. Furthermore, in [3] it is shown that the commutator map on finite simple groups is almost measure-preserving.

It seems likely that the strategy described above and developed in [6] can be used to complete the proof of Ore's conjecture, by dealing with the remaining cases, namely orthogonal and unitary groups. These present considerable additional technical difficulties, but work is under way and we hope to present a complete proof in a future paper.

References

[1] O. Bonten, Über Kommutatoren in endlichen einfachen Gruppen, Aachener Beiträge zur Mathematik, Bd. 7, Verlag der Augustinus-Buchhandlung, Aachen, 1993

[2] E.W. Ellers and N. Gordeev, On the conjectures of J. Thompson and O. Ore, *Trans. Amer. Math. Soc.* **350** (1998), 3657–3671.

[3] S. Garion and A. Shalev, Commutator maps, measure preservation, and T-systems, to appear in *Trans. Amer. Math. Soc.*

[4] R. Gow, Commutators in the symplectic group, *Arch. Math.* **50** (1988), 204–209.

[5] R. Gow, Commutators in finite simple groups of Lie type, *Bull. London Math. Soc.* **32** (2000), 311–315.

[6] M.W. Liebeck, E.A. O'Brien and A. Shalev, On the Ore conjecture, preprint.

[7] J. Neubüser, H. Pahlings and E. Cleuvers, Each sporadic finasig G has a class C such that $CC = G$, *Abstracts AMS* **34** (1984), 6.

[8] O. Ore, Some remarks on commutators, *Proc. Amer. Math. Soc.* **2** (1951), 307–314.

[9] A. Shalev, Word maps, conjugacy classes, and a non-commutative Waring-type theorem, to appear in *Annals of Math.*

[10] R.C. Thompson, Commutators in the special and general linear groups, *Trans. Amer. Math. Soc.* **101** (1961), 16–33.

[11] R.C. Thompson, On matrix commutators, *Portugal. Math.* **21** (1962), 143–153.

[12] R.C. Thompson, Commutators of matrices with coefficients from the field of two elements, *Duke Math. J.* **29** (1962), 367–373.

Maximal subgroups and irreducible restrictions

Pham Huu Tiep
(joint work with A. S. Kleshchev)

Finite primitive permutation groups have been studied since the pioneering work of Galois and Jordan on group theory; they have had important applications in many different areas of mathematics. If G is a primitive permutation group with a point stabilizer M then $M < G$ is a maximal subgroup. In most problems involving G, the Aschbacher-O'Nan-Scott theorem [AS] allows one to reduce to the case where G is an almost simple finite group, i.e. $L \lhd G \leqslant \mathrm{Aut}(L)$ for a non-abelian simple group L. The results of Liebeck, Praeger, and Saxl [LPS] and Liebeck and Seitz [LS] then allow one to assume furthermore that G is a finite classical group.

At this stage, Aschbacher's theorem [A] severely restricts possible choices of the maximal subgroup M. Namely, if $M < G$ is maximal then

$$M \in \bigcup_{i=1}^{8} \mathcal{C}_i \cup \mathcal{S},$$

where $\mathcal{C}_i$, $i = 1, \dots, 8$, are collections of certain explicit natural subgroups of G, and $\mathcal{S}$ is a collection of (almost simple) groups that act irreducibly on the natural module for the classical group G.

The converse however does not have to be true. So, to understand primitive permutation groups, one needs to determine whether a subgroup $M \in \cup_{i=1}^{8}\mathcal{C}_i \cup \mathcal{S}$ is actually maximal in G. For $M \in \cup_{i=1}^{8}\mathcal{C}_i$, this has been done by Kleidman and Liebeck [KL]. If a subgroup $M \in \mathcal{S}$ is *not* maximal then $M < N < G$ for a certain maximal subgroup N in G. It turns out that the most challenging case to understand is when $N \in \mathcal{S}$ as well. This leads to the following problem.

Problem 1. *Let $\mathbb{F}$ be an algebraically closed field of characteristic ℓ. Classify all triples (K, V, H), where K is a finite group with $K/Z(K)$ almost simple, V is an $\mathbb{F}K$-module of dimension greater than one, and H is a proper subgroup of K such that the restriction $V{\downarrow_H}$ is irreducible.*

Under the assumption $\ell > 3$, Problem 1 has been solved for the case where K is of alternating type, i.e. $K = \mathsf{A}_n, \mathsf{S}_n, \hat{\mathsf{A}}_n$ or $\hat{\mathsf{S}}_n$, see [BrK, KS2, KT], and many partial results are available even in the cases $\ell = 3$ and 2, see e.g. [KS1].

Now let us denote by Lie(p) the family of finite groups of Lie type whose defining fields have characteristic p. Definitive results on Problem 1 in the case where

$K \in \mathrm{Lie}(\ell)$ have been obtained by Liebeck, Seitz, and Testerman [L], [S1], [ST]. On the other hand, ongoing work of Magaard, Röhrle, Testerman [MRT] essentially reduces the case $H \in \mathrm{Lie}(\neq \ell)$ to the following problem:

Problem 2. *Let G be a Zariski closed subgroup of a simple classical group $\mathcal{G} = Cl(W)$, and let V be the largest composition factor of the $\mathcal{G}$-module $W \otimes W^*$, $Sym^k(W)$, or $\wedge^k(W)$, with k "small". When can $V \downarrow_G$ be irreducible?*

This problem in the case V comes from $W \otimes W^*$, $Sym^2(W)$, $\wedge^2(W)$ has been treated by Magaard, Malle, and the speaker [M, MM, MMT]. On the other hand, the case $V = Sym^k(W)$ with $k \geq 4$ is known as the *Kollár-Larsen Problem* [BK]: *Which closed subgroups of $GL(W)$ are irreducible on some symmetric power of W?*

The Kollár-Larsen problem is largely motivated by its applications in algebraic geometry, cf. the recent work of Balaji and Kollár [BK] on the holonomy groups of vector bundles on a smooth projective variety. This problem has now been essentially solved by Guralnick and the speaker.

Theorem 3. [GT]. *Assume a Zariski closed subgroup G of $\mathcal{G} := GL(W)$ acts irreducibly on $Sym^k(W)$ for some $k \geq 4$. Then one of the following holds.*

(i) *$\mathcal{H} \lhd G \leqslant N_{\mathcal{G}}(\mathcal{H})$ with $\mathcal{H} \in \{SL(W), Sp(W)\}$.*

(ii) *$\ell > 0$, $L \lhd G \leqslant N_{\mathcal{G}}(L)$, where $L = SL_d(q)$, $SU_d(q)$, or $Sp_d(q)$, $q = \ell^a$ and $d = \dim(W)$.*

(iii) *$k = 4, 5$, and $L \lhd G \leqslant N_{\mathcal{G}}(L)$, with $(\dim(W), L) = (6, 2J_2)$, $(12, 2G_2(4))$, $(12, 6Suz)$.*

(iv) *$k = 4, 5$, $\ell = 5, 7$, and $M \lhd G \leqslant N_{\mathcal{G}}(M)$, with $M =$ Monster.*

What happens when $k \leqslant 3$ is partially addressed in the following result of Magaard and the speaker:

Theorem 4. [MT2] *Let $G = Sp_{2n}(3)$ with $n \geq 3$, and let η, ξ be (associated) Weil characters of degree $(3^n - 1)/2$, resp. $(3^n + 1)/2$. Then*

$$Sym^3(\eta),\ \wedge^3(\xi),\ \eta \otimes Sym^2(\xi),\ \xi \otimes \wedge^2(\eta)$$

are all irreducible.

Note that, until very recently, known infinite series of examples of irreducible tensor squares, symmetric or alternating squares, cf. [MT1, M, MMT], have all the involved factors being Weil representations of finite symplectic or unitary groups.

We will now focus on the *cross characteristic* case, that is the case where $K \in \mathrm{Lie}(p)$ with $p \neq \ell$. When G is classical group, Seitz's theorem [S2] lists possible candidates for the subgroup H arising in Problem 1 under the condition that $H \in \mathrm{Lie}(p)$.

Note that for the purposes of Aschbacher's program, it suffices to solve Problem 1 in the case where $K/Z(K)$ is almost simple. However, for K of Lie type A, just like for K of alternating type, it turns out to be possible, and more convenient, to solve Problem 1 in full generality. We believe that this might be of importance for various applications in group theory.

Let q be a prime power. The main results of the paper deal with Problem 1 in the case where K is of Lie type A over a field with q elements, i.e. $SL_n(q) \leqslant K \leqslant GL_n(q)$, and $\ell \not| \, q$. In the following theorem, we use the James' labeling of irreducible $\mathbb{F}G$-modules [J], see also [BDK, 4.4b].

Theorem 5. *Let $SL_n(q) \leqslant K \leqslant GL_n(q)$. Assume that $H < K$ is a proper subgroup not containing $SL_n(q)$, W is an absolutely irreducible representation of $GL_n(q)$ in characteristic $\ell \not| q$ with $\dim(W) > 1$, and V is an irreducible constituent of W restricted to K. If $V{\downarrow}_H$ is irreducible then one of the following holds:*

(i) *$H \leqslant P \cap K$, where P is the stabilizer in $GL_n(q)$ of a 1-space or an $(n-1)$-space in the natural $GL_n(q)$-module $\mathbb{F}_q^n$, and $W = L(t,(k))$ for some element t of degree $n/k > 1$.*

(ii) *n is even, $W = L(s,(1)) \circ L(t,(n-1))$ for some ℓ'-elements $s, t \in \mathbb{F}_q^\times$ with $t \not\sim s$; in particular, $V = W{\downarrow}_K$ and $\dim(V) = (q^n-1)/(q-1)$. Furthermore, either $Sp_n(q) \leqslant H \leqslant CSp_n(q)$, or $2|q$ and $G_2(q)' \lhd H \leqslant GL_n(q)$. Moreover, such a module V is irreducible over $Sp_n(q)$ precisely when $t \not\sim \pm s$.*

(iii) *One of eight cases, with $(n,q) = (4,2)$, $(3,4)$, $(3,2)$, $(n = 2, 3 \leqslant q \leqslant 11)$, occurs.*

One of the key ingredients in the proof of prove Theorem 5 is a description of the irreducible representations of $GL_n(q)$ that are irreducible over $SL_n(q)$, a result which seems to be of an independent interest (a similar problem of classifying modular representations of S_n that are irreducible over A_n was solved in [B] and [FK]).

A partition λ is called *ℓ-divisible* if ℓ divides all parts of the transposed partition λ'.

Theorem 6. *Let $V = L(\sigma_1, \lambda^{(1)}) \circ \ldots \circ L(\sigma_m, \lambda^{(m)})$ be an irreducible $\mathbb{F}GL_n(q)$-representation, where the σ_i are ℓ'-elements. Then $V{\downarrow}_{SL_n(q)}$ is reducible if and only if at least one of the following holds:*

(i) *There is some ℓ'-element $1 \neq t \in \mathbb{F}_q^\times$ such that, for all $i = 1, \ldots, m$, the set $\{\sigma_j \mid 1 \leqslant j \leqslant m, \ \lambda^{(j)} = \lambda^{(i)}\}$ is stable under the multiplication by t.*

(ii) *$\ell | \gcd(n, q-1)$, and $\lambda^{(i)}$ is ℓ-divisible for all i.*

Acknowledgements. The author gratefully acknowledges the support of the NSF.

References

[A] M. Aschbacher, *On the maximal subgroups of the finite classical groups*, Invent. Math. **76** (1984), 469–514.

[AS] M. Aschbacher and L. Scott, *Maximal subgroups of finite groups*, J. Algebra **92** (1985), 44–80.

[B] D. Benson, *Spin modules for symmetric groups*, J. London Math. Soc. **38** (1988), 250–262.

[BK] V. Balaji and J. Kollár, *Holonomy groups and stable vector bundles*, preprint (arXiv:math.AG/0601120).

[BrK] J. Brundan and A. Kleshchev, *Representations of the symmetric group which are irreducible over subgroups*, J. reine angew. Mathematik, **530** (2001), 145–190.

[BDK] J. Brundan, R. Dipper, and A. S. Kleshchev, *Quantum linear groups and representations of $GL_n(\mathbb{F}_q)$*, Memoirs Amer. Math. Soc. **149** (2001), No. 706.

[FK] B. Ford and A. S. Kleshchev, *A proof of the Mullineux conjecture*, Math. Z. **226** (1997), 267–308.

[GT] R. M. Guralnick and Pham Huu Tiep, *Symmetric powers and a problem of Kollár and Larsen*, (submitted).

[J] G. James, *The irreducible representations of the finite general linear groups*, Proc. London Math. Soc. **52** (1986), 236–268.

[KL] P. B. Kleidman and M. W. Liebeck, '*The Subgroup Structure of the Finite Classical Groups*', London Math. Soc. Lecture Note Ser. no. **129**, Cambridge University Press, 1990.

[KS1] A. Kleshchev and J. Sheth, *Representations of the symmetric group are reducible over simply transitive subgroups*, Math. Z. **235** (2000), 99–109.

[KS2] A. Kleshchev and J. Sheth, *Representations of the alternating group which are irreducible over subgroups*, Proc. London Math. Soc. **84** (2002), 194–212.

[KT] A. Kleshchev and Pham Huu Tiep, *On restrictions of modular spin representations of symmetric and alternating groups*, Trans. Amer. Math. Soc. **356** (2004), 1971–1999.

[L] M. W. Liebeck, *On the orders of maximal subgroups of the finite classical groups*, Proc. London Math. Soc. **50** (1985), 426–446.

[LPS] M. W. Liebeck, C. Praeger, and J. Saxl, *A classification of the maximal subgroups of the finite alternating groups and symmetric groups*, J. Algebra **111** (1987), 365–383.

[LS] M. W. Liebeck and G. M. Seitz, *On finite subgroups of exceptional algebraic groups*, J. reine angew. Math. **515** (1999), 25–72.

[MM] K. Magaard, G. Malle, *Irreducibility of alternating and symmetric squares*, Manuscripta Math. **95** (1998), 169–180.

[M] G. Malle, *Almost irreducible tensor squares*, Comm. Algebra **27** (1999), 1033–1051.

[MMT] K. Magaard, G. Malle and Pham Huu Tiep, *Irreducibility of tensor squares, symmetric squares, and alternating squares*, Pacific J. Math. **202** (2002), 379–427.

[MRT] K. Magaard, G. Röhrle, and D. Testerman, (in preparation).

[MT1] K. Magaard and Pham Huu Tiep, *Irreducible tensor products of representations of finite quasi-simple groups of Lie type*, in: 'Modular Representation Theory of Finite Groups', M. J. Collins, B. J. Parshall, L. L. Scott, eds., Walter de Gruyter, Berlin et al, 2001, pp. 239–262.

[MT2] K. Magaard and Pham Huu Tiep, (in preparation).

[S1] G. M. Seitz, *The maximal subgroups of classical algebraic groups*, Memoirs Amer. Math. Soc. **67** (1987), no. 365.

[S2] G. M. Seitz, *Cross-characteristic embeddings of finite groups of Lie type*, Proc. London Math. Soc. **60** (1990), 166–200.

[ST] G. M. Seitz and D. Testerman, *Extending morphisms from finite to algebraic groups*, J. Algebra **131** (1990), 559–574.

The generation of the augmentation ideal

Erika Damian

In [6] the following observation is made: an abstract group H is finitely generated if and only if the augmentation ideal of $\mathbb{Z}[H]$ is a finitely generated module over the group algebra $\mathbb{Z}[H]$; it is probably not known whether such a statement is true for profinite groups (with $\hat{\mathbb{Z}}[-]$ instead of $\mathbb{Z}[-]$). We show that in general the answer to this question is negative. We find a formula for $d_{\hat{\mathbb{Z}}[[G]]}(I[[G]])$, the minimum number of generators of the augmentation ideal as a $\widehat{\mathbb{Z}}[[G]]$-module, where G is a profinite group and $\widehat{\mathbb{Z}}[[G]]$ is the completed group algebra of G over the profinite ring $\widehat{\mathbb{Z}}$, which extends that obtained in [1] in the finite setting.

Theorem 1. *Let G be a profinite group and assume that $I[[G]]$ is a finitely generated $\widehat{\mathbb{Z}}[[G]]$-module. Then*

$$d_{\widehat{\mathbb{Z}}[[G]]}(I[[G]]) = \max_{p\ prime} \max_{M \in \mathrm{Irr}(\mathbb{Z}/p\mathbb{Z}[[G]])} \left\lceil \frac{s_M + r_M \zeta_M}{r_M} \right\rceil$$

where $\mathrm{Irr}(\mathbb{Z}/p\mathbb{Z}[[G]])$ is a set of representatives of finite and irreducible $\mathbb{Z}/p\mathbb{Z}[[G]]$-modules; $s_M = \dim_{\mathrm{End}_G(M)} H^1(G, M)$; $r_M = \dim_{\mathrm{End}_G(M)} M$ and ζ_M is 0 when M is trivial and 1 otherwise.

This formula allows us to show as a counterexample to the above statement a profinite group which is not finitely generated (in the topological sense) such that the augmentation ideal is 2-generated as a $\widehat{\mathbb{Z}}[[G]]$-module. On the other hand we extend a result which holds for finite solvable groups (see [2]) by proving that in the prosolvable case the minimum number of generators of a prosolvable group coincides with the minimal number of generators of the augmentation ideal as a module over the completed group algebra.

We then further our investigation and tackle probabilistic questions concerning the generation of the augmentation ideal $I[[G]]$ of a profinite group G; by definition $I[[G]]$ is the kernel of the augmentation map $\epsilon : \widehat{\mathbb{Z}}[[G]] \to \widehat{\mathbb{Z}}$ which maps each element of G to 1. Since the completed group algebra $\widehat{\mathbb{Z}}[[G]]$ is a profinite ring we may consider the normalized Haar measure on it so that it becomes a probabilistic space. In this setting we define for any $k \in \mathbb{N}$ the probability $\mathrm{Prob}_{\widehat{\mathbb{Z}}[[G]]}(I[[G]], k)$ of generating the $\widehat{\mathbb{Z}}[[G]]$-module $I[[G]]$ with k random elements as the measure of the set of k-tuples which generate $I[[G]]$ as a $\widehat{\mathbb{Z}}[[G]]$-module. For $k \geq d_{\widehat{\mathbb{Z}}[[G]]}(I[[G]])$, we find a formula for this probability which can be written as an infinite product indexed over the irreducible G-modules in characteristic p where p ranges over the set of all prime numbers.

Theorem 2. *Let G be a profinite group and assume that the augmentation ideal $I[[G]]$ is d-generated. Then for $k \geq d$ we get that*

$$\mathrm{Prob}_{\widehat{\mathbb{Z}}[[G]]}(I[[G]], k) = \prod_{p} \prod_{M \in \mathrm{Irr}(\mathbb{Z}/p\mathbb{Z}[[G]])} \prod_{i=0}^{s_M + r_M\zeta_M - 1} \left(1 - \frac{|\operatorname{End}_{\mathbb{Z}/p\mathbb{Z}[[G]]}(M)|^i}{|M|^k}\right)$$

We study the class of profinite groups for which the augmentation ideal is generated with positive probability for some positive integer (i.e. when the infinite product above converges for some positive integer); we call this class APFG (Augmentation Positive Finitely Generated). First we find a useful characterization for this class of profinite groups:

Theorem 3. *Let G be profinite group and assume that the augmentation ideal is finitely generated as a $\widehat{\mathbb{Z}}[[G]]$-module. G is APFG if and only if the number of irreducible G-modules of finite order is polynomially bounded as a function of the order.*

This characterization allows us to prove that the class of PFG groups is contained in the class of APFG groups; the proof of this result employs different characterizations of PFG groups, see [5], [4] and [3]. However these two classes do not coincide: we give an example of a 2-generated APFG group which is not PFG.

References

[1] John Cossey, K. W. Gruenberg, and L. G. Kovács, *The presentation rank of a direct product of finite groups*, J. Algebra **28** (1974), 597–603. MR MR0424969 (54 #12927)

[2] Karl W. Gruenberg, *Relation modules of finite groups*, American Mathematical Society, Providence, R.I., 1976, Conference Board of the Mathematical Sciences Regional Conference Series in Mathematics, No. 25. MR MR0457538 (56 #15743)

[3] A. Jaikin-Zapirain and L. Pyber, *Random generation of finite and profinite groups and group enumeration*, preprint.

[4] Avinoam Mann, *Positively finitely generated groups*, Forum Math. **8** (1996), no. 4, 429–459. MR 97j:20029

[5] Avinoam Mann and Aner Shalev, *Simple groups, maximal subgroups, and probabilistic aspects of profinite groups*, Israel J. Math. **96** (1996), no. , part B, 449–468. MR 97m:20038

[6] Thomas Weigel, *On the probabilistic ζ-function of pro(finite-soluble) groups*, Forum Math. **17** (2005), no. 4, 669–698. MR MR2154424 (2006c:20061)

Proper vertex colourings and graph automorphisms

Jason D. Rudd

1. The Orbital Chromatic Polynomial

Given a graph Γ, a *proper k-vertex colouring*, or *colouring* for short of Γ is an assignment of colours from a set of k colours to the vertices of Γ with the condition that no two adjacent colours receive the same colour.

We are interested in the number of colourings of various graphs, so let $\chi(\Gamma; k)$ denote the number of colourings of the graph Γ that are possible from from k colours. It is easy to see that if $\Gamma \setminus e$ is a graph Γ with an edge e deleted and Γ/e is Γ with e contracted, then $\chi(\Gamma \setminus e; k) = \chi(\Gamma/e; k) + \chi(\Gamma; k)$ because $\chi(\Gamma/e; k)$ gives the number of colourings of $\Gamma \setminus e$ with the same colour on the vertices at either end of e, and $\chi(\Gamma; k)$ gives the number of colourings of $\Gamma \setminus e$ with different colours on the vertices at either end of e. This gives us that

$$\chi(\Gamma; k) = \chi(\Gamma \setminus e; k) - \chi(\Gamma/e; k)$$

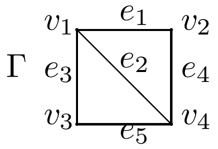
which means that Γ can be decomposed into a series of empty graphs. The number of colourings of an empty graph on n vertices from k colours is clearly k^n, so $\chi(\Gamma; k)$ must be a polynomial, which we call the *chromatic polynomial.* Note that contraction may lead to a graph having a loop, and that for any graph with a loop, the chromatic polynomial is identically zero.

Suppose that we want to know the number of colourings of a graph Γ up to some symmetry of Γ. That is, if $G \leqslant \mathrm{Aut}(\Gamma)$ is an automorphism group of Γ, the number of orbits of G on colourings of Γ. The main tool here is the *orbit counting lemma*, $\#$ orbits $= \frac{1}{|G|}\sum_{g\in G}\mathrm{fix}(g)$, where $\mathrm{fix}(g)$ is the number of colourings fixed by the automorphism g. With this in mind, all that needs to be calculated is the number of colourings fixed by each $g \in G$.
If Γ is a graph and g is an automorphism of Γ, let Γ/g be the graph obtained from Γ in which the vertices correspond to the cycles of g on vertices of Γ and the edges correspond to the cycles of g on edges of Γ, where incidence is preserved from Γ to Γ/g. Note that if two adjacent vertices lie in the same g vertex cycle, Γ/g will have a loop.

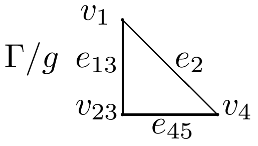
The number of colourings of Γ fixed by g is given by the number of colourings of the graph Γ/g: if a colouring is fixed then every vertex in a given g-vertex cycle must have the same colour, and two vertices of Γ are adjacent if and only if their images in Γ/g are adjacent. Therefore the number of orbits of G on k colourings of Γ is also a polynomial in k, which we call the *Orbital Chromatic Polynomial*, and can be defined by

$$O\chi(\Gamma, G; k) = \frac{1}{|G|}\sum_{g\in G}\chi(\Gamma/g; k)$$

Example.



$g = (v_2v_3) = (e_1e_3)(e_4e_5)$



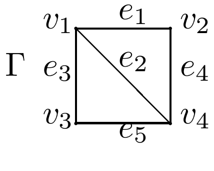
If Γ and g are as above, and $G = \{\mathrm{id}, g\}$, the orbital chromatic polynomial is given by

$$O\chi(\Gamma, G; k) = \frac{1}{2}[k(k-1)(k-2)^2 + k(k-1)(k-2)] = \frac{1}{2}k(k-1)^2(k-2)$$

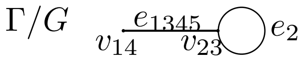
2. The Fixed Point Chromatic Polynomial

In the next section it will be necessary to find out, given a graph Γ and an automorphism group $G \leqslant \mathrm{Aut}(\Gamma)$, how many colourings of Γ are fixed by every $g \in G$. Let Γ/G be the graph obtained from Γ in which the vertices correspond to the G-vertex orbits and the edges to the G-edge orbits, where incidence is preserved from Γ to Γ/G.

Example.



$G = \{\mathrm{id}, (v_2v_3), (v_1v_4), (v_1v_4)(v_2v_3)\}$



As in the previous section it is clear that the number of colourings of Γ fixed by every $g \in G$ is given by the chromatic polynomial of Γ/G, which we call the *Fixed Point Chromatic Polynomial*

$$\mathrm{FP}\chi(\Gamma, G; k) = \chi(\Gamma/G; k)$$

In the above example, there are never any colourings of Γ fixed by every $g \in G$, whatever the value of k.

3. Sizes of G-Orbits

We have already seen how to count the number of orbits of G on colourings of Γ. In this section we look at how to calculate the sizes of these orbits, that is, to find the number of orbits of a given size.

In general, if G is a permutation group acting on a set Ω, for $\alpha \in \Omega$, the *stabiliser* G_α in G of α is the maximal subgroup $H \leqslant G$ such that every $h \in H$ fixes α. For a subgroup $H \leqslant G$, let $M(H) \subseteq \Omega$ be the maximal subset of Ω such that H is the stabiliser of every $\alpha \in M(H)$. For $H_1, H_2 \leqslant G$ $(H_1 \neq H_2)$, it is easy to see that the sets $M(H_1)$ and $M(H_2)$ are disjoint. If not, then $\exists \beta \in M(H_1) \cap M(H_2)$ in which case β is fixed by every element of the group $\langle H_1, H_2 \rangle$. Thus H_1 is not maximal with respect to fixing β, and so is not the stabiliser of β, which is a contradiction: $M(H_1)$ and $M(H_2)$ must be disjoint.

Using Möbius inversion, it can be shown that, if G is a permutation group acting on a set Ω, and $H \leqslant G$; the number of elements of Ω for which H is the stabiliser is given by

$$|M(H)| = \sum_{(G\geq)J\geq H} \mu(H,J)\mathrm{fix}(J) \qquad \mu(H,J) = \begin{cases} 1 & H = J \\ 0 & H \nleqslant J \\ -\displaystyle\sum_{J\geq K>H} \mu(K,J) & H \leqslant J \end{cases}$$

(μ is the Möbius function on the poset of subgroups of G, ordered by inclusion, and $\mathrm{fix}(J)$ is the number of elements of Ω fixed by every $j \in J$.)

A well known result of permutation group theory gives us that if H is the stabiliser of $\alpha \in \Omega$, then the index $|G|/|H|$ of H in G is equal to the size of the orbit containing α.

Now we can calculate the numbers of elements of Ω with stabilisers of each index, and hence the sizes of the orbits. Clearly

$$\#\text{ orbits of size } n = \frac{\left[\begin{array}{l} \#\text{ elements lying in orbits of size } n \\ = \#\text{ elements with stabilisers of index } n \end{array}\right]}{n}$$

When considering colourings the set Ω is the set of colourings of Γ, and for $J \leqslant G \leqslant \mathrm{Aut}(\Gamma)$, $\mathrm{fix}(J)$ is just $\chi(\Gamma/J)$.

Thus the ordinary generating function for the size of the orbits of G on the colourings of Γ is

$$f_G(t) = \frac{1}{|G|} \sum_{H \leqslant G} |H| t^{|G|/|H|} \sum_{(G \geq) J \geq H} \mu(H,J)\chi(\Gamma/J)$$

Example. Let Γ and G be the graph and automorphism group from the previous example. The subgroups of G are G, $\{\mathrm{id}, (v_2v_3)\}$, $\{\mathrm{id}, (v_1v_4)\}$, $\{\mathrm{id}, (v_1v_4)(v_2v_3)\}$, and $\{\mathrm{id}\}$. A bit of fairly involved calculation gives the generating function for the sizes of the orbits in this case as

$$f_G(t) = \frac{1}{4}\left[2t^2k(k-1)(k-2) + t^4k(k-1)(k-2)(k-3)\right]$$

so that there are $\frac{1}{2}k(k-1)(k-2)$ orbits of size 2 and $\frac{1}{4}k(k-1)(k-2)(k-3)$ orbits of size 4.

References

[1] P.J. Cameron, *Permutation Groups* (1999) LMS Student Texts 45, Cambridge University Press.

[2] B. Bollobás, *Modern Graph Theory* (1998) GTM 184, Springer-Verlag, New York.

[3] P.J. Cameron, B. Jackson, and J.D. Rudd, *Orbit-counting polynomials for graphs and codes* (2005), submitted to Discrete Mathematics.

[4] J.D. Rudd *Tutte polynomials for counting and classifying orbits*(2007), submitted to Discrete Mathematics.

The divisor matrix and SL$(2,\mathbb{Z})$

John G. Thompson

The divisor matrix is

$$D = (d_{ij})_{(i,j)\in\mathbb{N}\times\mathbb{N}},$$

$$d_{ij} = \begin{cases} 1 & \text{if } i|j \\ 0 & \text{if } i \nmid j \end{cases}$$

Set

$$G = \mathrm{GL}\,(\mathbb{N},\mathbb{Q}) = BNB$$

where B is the group of upper triangular matrices over $\mathbb{Q}$, indexed by $\mathbb{N}\times\mathbb{N}$ with non-zero entries on the diagonal and N is the group of matrices over $\mathbb{Q}$ indexed by $\mathbb{N}\times\mathbb{N}$, with precisely one nonzero entry in each row and column. Set $V = \mathbb{Q}^{\mathbb{N}}$, so that G acts on V in the usual way.

Theorem 1. *There is a subgroup S of G and an isomorphism $\varphi : \mathrm{SL}\,(2,\mathbb{Z}) \to S$ such that*

(i) $\varphi((\begin{smallmatrix}1&1\\0&1\end{smallmatrix})) = D$

(ii) $S \subseteq \mathrm{GL}\,(\mathbb{N},\mathbb{Z})$

(iii) *If W is any composition factor of S on V, then S acts faithfully on W and* $\dim W = 2$.

Recognizing the alternating and the symmetric groups from their probabilistic zeta function

Andrea Lucchini

For any finite group G we may define a sequence of integers $\{a_n(G)\}_{n\in\mathbb{N}}$ as follows:

$$\forall n \in \mathbb{N} \qquad a_n(G) = \sum_{|G:H|=n} \mu_G(H).$$

Here μ_G is the Möbius function defined on the subgroup lattice $L(G)$ of G. Let

$$P_G(s) = \sum_{n\in\mathbb{N}} \frac{a_n(G)}{n^s}$$

be the Dirichlet generating function associated with the sequence $\{a_n(G)\}_{n\in\mathbb{N}}$. For any $t \in \mathbb{N}$, $P_G(t)$ gives the probability that t randomly chosen elements of G generate G. Since $\mu_G(H) \neq 0$ only if H is an intersection of maximal subgroups of G, the series $P_G(s)$ can be viewed as a way of encoding in a compact way information concerning the sublattice of $L(G)$ generated by the maximal subgroups of G. It is quite natural to investigate what may be recovered about the group $G/\operatorname{Frat}(G)$ from the Dirichlet series $P_G(s)$.

Suppose that G is a finite simple group and let H be a finite group with $\operatorname{Frat} H = 1$ and $P_G(s) = P_H(s)$. It was proved in [1] that H is simple. The following criterion can be applied:

Theorem 1. *Let $m = \min\{n > 1 \mid a_n(G) \neq 0\}$. The factor group $G/\operatorname{Frat} G$ is simple and nonabelian if and only if the following conditions are satisfied:*

(i) *if $a_n(G) \neq 0$ then n divides $m!$*

(ii) *if $q = p^r$ is a prime-power and $a_q(G) \neq 0$, then $a_q(G) \equiv 0 \bmod p$ and either $q = m$ or $(q, m) = (8, 7)$;*

(iii) *n divides $a_n(G) \forall n \in \mathbb{N}$ and $\prod_{n\ odd} n^{\frac{a_n(G)}{n}} \neq 1$.*

It can be conjectured that the stronger result $G \cong H$ holds and this conjecture has been verified in several cases (see [2]). A proof of this conjecture in the case when G is the alternating group has been obtained in [3], using the classification of 2-transitive permutation groups. Recently we obtained a new, simpler proof in which the only property of finite simple groups that is used is the solvability of the outer automorphism group and that gives also an easy criterion to decide from the series $P_G(s)$ whether $G/\operatorname{Frat} G \cong \operatorname{Alt}(m)$.

Theorem 2. *Let $P_G(s) = \sum_{n\in\mathbb{N}} a_n/n^s$. Then $G/\operatorname{Frat} G \cong \operatorname{Alt}(m)$ if and only if the following properties are satisfied:*

(i) *$m = \min\{n \in \mathbb{N} \mid n > 1$ and $a_n \neq 0\}$;*

(ii) *for any $n \in \mathbb{N}$, if $a_n \neq 0$ then n divides $\frac{m!}{2}$;*

(iii) *if q is a prime and $a_q \neq 0$, then $q = m$ and $a_q = -q$;*

(iv) *for any prime $p \leqslant m$, there exists n that $a_n \neq 0$ and p divides n;*

(v) *for any $n \in \mathbb{N}$, n divides a_n and $\prod_{n\ odd} n^{\frac{a_n}{n}} \neq 1$.*

Similar methods (but a more intensive use of the classification of finite simple groups) allow us to prove:

Theorem 3. *If* $P_G(s) = P_{\mathrm{Sym}(n)}(s)$ *and* $\mathrm{Frat}\, G = 1$*, then either* $G = \mathrm{Sym}(n)$ *or* $G = \mathrm{Alt}(n) \times C_2$.

Note that $P_{\mathrm{Sym}(n)}(s) = P_{\mathrm{Alt}(n)\times C_2}(s)$ for $n = 2, 5, 6$ but not for $n = 3, 4, 7, 8, 9$. These phenomena seem to reflect the existence (or non-existence) of maximal subgroups of $\mathrm{Alt}(n)$ whose normalizer is a maximal subgroup of $\mathrm{Sym}(n)$. However a precise result in this direction is still missing.

References

[1] Erika Damian and Andrea Lucchini, *The probabilistic zeta function of finite simple groups*, J. Algebra, **313** (2007), 957-971.

[2] Erika Damian and Andrea Lucchini, *On the Dirichlet polynomial of finite groups of Lie type*, Rend. Sem. Mat. Univ. Padova **115** (2006), 51–69.

[3] Erika Damian and Andrea Lucchini, *Recognizing the alternating groups from their probabilistic zeta function*, Glasg. Math. J. **46** (2004), 595–599.

The root groups of special Moufang sets

Yoav Segev

Recall that a Moufang set is a doubly transitive permutation group G on a set X, $|X| \geq 3$, such that the point stabilizer G_x contains a normal subgroup U_x (called the root group) which is regular on the remaining points and whose conjugates generate G.

This talk is concerned with the following conjecture.

Conjecture. *Let* $\mathbb{M}(U, \tau)$ *be a special Moufang set, then* U *is abelian.*

The notation $\mathbb{M}(U, \tau)$ as well as the definition of "special" is explained in [DS1]. See also [DS2] for further information about Moufang sets. Throughout the rest of this talk summary, let $\mathbb{M}(U, \tau)$ be a special Moufang set. Then U enjoys the following properties.

Properties of U.

(i) ([SW]) Either U is a group of exponent 2 or $H := G_{0,\infty}$ acts "irreducibly" on U (i.e. U contains no proper nontrivial H-invariant subgroup). In particular

(ii) U is characteristically simple.

(iii) ([DS1]) For all $a \in U^*$, $|a| = \infty$ or $|a|$ is a prime.

(iv) ([DS1]) If $1 < n < |a|$ ($a \in U^*$) then a has a unique n-th root in U. From (iii) and (iv) it follows that

(v) For $a \in U^*$, $C_U(a)$ is either a torsion-free uniquely divisible group or a group of exponent p for some prime p. In particular

(vi) (See [T].) If U is abelian then U is an $\mathbb{F}$-vector space, where $\mathbb{F} = \mathbb{Q}$ or $\mathrm{GF}(p)$.

(vii) ([DST]) If U contains involutions then U is a group of exponent 2.

(viii) (Follows from the classification of finite Moufang sets, see [HKS].) If U is finite then U is an elementary abelian p-group, for some prime p.

(ix) ([DST]) If U contains an element of finite order p, then any element of U is a product of two elements of order p.

Properties (i)–(ix) do not imply that U is abelian in general. To further restrict the structure of U we introduce certain relations that hold amongst certain elements of U. These relations are obtained using properties of the μ-maps.

Basic relations.

Let $a, b \in U^*$ and set $z := a\mu_b$. Let $1 \leq n < |a|$ and recall that we are writing U with additive notation though we are not assuming that U is commutative. Further for $x \in U^*$ and an integer m such that $1 \leq m < |x|$, $x \cdot m$ denotes the m-th power of x and $x \cdot \frac{1}{m}$ denotes the m-th root of x. Set

$$y_n := (-b - a \cdot n + z \cdot \tfrac{1}{n} - b) \cdot n.$$

Here are some relations that hold in U which we call the basic relations (see [DST]).

(BR1) $|a| = |z| = \left|-b - a \cdot n + z \cdot \frac{1}{n} - b\right|$.

(BR2) For all integers m such that $1 \leq |m| < |a|$,

$$\begin{aligned}&(-b - a \cdot mn + z \cdot \tfrac{1}{mn} - b) \cdot n = \\ &- b - a \cdot mn - b - a \cdot m(n-1) - \cdots - b - a \cdot m + z \cdot \tfrac{1}{n} \\ &- b - b - a \cdot m - b - a \cdot 2m - \cdots - b - a \cdot m(n-1).\end{aligned}$$

(BR3) For $1 \leq r, s < |a|$ such that $n \equiv r + s \pmod{|a|}$ (so $n = r + s$ if $|a| = \infty$),

$$y_n = (-b - a \cdot n + y_s \cdot \tfrac{1}{r} - b - a \cdot s) \cdot r.$$

(BR4) The relations (BR1)–(BR3) hold with b and $-b$ interchanged as well as a and z interchanged.

We hope that some elaboration on the above basic relations together with the properties of U, and in particular property (ix), will lead to a proof that if U contains an element of finite order p then U is a group of exponent p.

The case where U is finite.

Toward the end of my talk I gave a sketch of a direct proof of the known fact that when U is finite, then it is abelian (property (viii)). The proof comes from [S]. So assume that U is finite but that U is not abelian, and choose $\mathbb{M}(U, \tau)$ with $|U|$ minimal. By property (vii), $|U|$ is odd. If we use the Feit-Thompson Odd Order Theorem, then U is solvable and together with property (ii) this implies that U is abelian, a contradiction. Without using the Odd Order Theorem the proof is obtained roughly using the following steps.

Step 1. Show that H $(= G_{0,\infty})$ has a unique class of involutions.

Step 2. Deduce that there exists a unique prime p such that if μ_a is not an involution, then $|a| = p$. This uses a theorem in [DST] that says that if μ_a is an involution for all $a \in U^*$, then U is abelian.

Step 3. Let p be the prime of Step 2. Let P be a nontrivial p-subgroup of U and let $y \in U^*$ be an element of order $q \neq p$ in $N_U(P)$. Then the elements y, $-x + y + x$, $y + x$ and $-y + x$ all have order q, so, by Step 2, μ_a is an involution, for $a \in \{y, -x + y + x, y + x, -y + x\}$. By a lemma in [DST] this implies that x and y commute, contradicting propety (iii) of U. Hence $N_U(P)$ is a p-group. By the Frobenious normal p-complement theorem U has a normal p-complement, contradicting property (ii) of U.

Remark. I thank Bill Kantor (and later also Alexander Stein) for bringing to my attention the fact that the proof of the statement: Let K be a finite group of odd order such that the order of each nonidentity element in K is a prime number. Then K is solvable; does not require the full strength of the Odd Order Theorem. Of course the paper [FHT] suffices. Thus, to prove that if U is finite of odd order, then U is abelian it suffices (by properties (ii) and (iii) of U) to use [FHT]. However, the proof in [S] that if $|U|$ is odd then U is abelian is still more elementary (and maybe parts of it extend to the case where U is infinite).

References

[DS1] T. De Medts, Y. Segev, *Identities in Moufang sets,* to appear in Trans. Amer. Math. Soc. (http://cage.ugent.be/ tdemedts/preprints/ystd05.pdf)

[DS2] T. De Medts, Y. Segev, *A course on Moufang sets,* submitted to Innovations in Incidence Geometry. (http://cage.ugent.be/ tdemedts/preprints/moufsets.pdf)

[DST] T. De Medts, Y. Segev, K. Tent, *Special Moufang sets, their root groups and their μ-maps,* to appear in Proc. London Math. Soc. (http://cage.ugent.be/ tdemedts/preprints/tdyskt06-lms.pdf)

[FHT] W. Feit, M. Hall, Jr., J. G. Thompson, *Finite groups in which the centralizers of any nonidentity element is nilpotent,* Math. Z. **74** (1960), 1–17.

[HKS] C. Hering, W. M. Kantor, G. M. Seitz, *Finite groups with a split BN-pair of rank* 1*, I,* J. Algebra **20** (1972), 435–475.

[S] Y. Segev, *Finite special Moufang sets of odd characteristic,* submitted.

[SW] Y. Segev, R. M. Weiss, *On the action of the Hua subgroups in special Moufang sets*, to appear in Math. Proc. Cambridge Philos. Soc.

[T] F. Timmesfeld, *Abstract Root Subgroups and Simple Groups of Lie-Type*, Birkhäuser-Verlag, Monographs in Mathematics **95**(2001), Basel, Berlin, Boston.

Automorphisms and Weierstrass points of curves

Kay Magaard
(joint work with Helmut Völklein)

Let X_g be a compact, connected, Riemannn surface, or curve for short, of genus $g \geq 2$. A point $x \in X$ is a **Weierstrass point** if X posesses a meromorphic function which has a pole of order $\leq g$ at x and is holomorphic on $X \setminus x$. We denote the set of Weierstrass points of X by $\mathcal{W}(X)$ and the automorphism group by G. If $h \in G$ we denote the fixed points of h on X by $F_X(h)$.

Lemma 1. *(Schöneberg) If $|F_X(h)| \geq 5$, then $F_X(h) \subset \mathcal{W}(X)$.*

Define $S := \cup_{h \in G} F_X(h)$. It is well known that $S = \cup_{i=1}^{r} \Pi^{-1}(y_i)$, where $\Pi : X \longrightarrow X/G$ is the natural projection and $y_1, \ldots, y_r \in X/G$ are the branch points of Π. Furthermore if $x_i \in \Pi^{-1}(y_i)$ then the stabilizer of x_i is $G_{x_i} = \langle h_i \rangle$, i.e. cyclic. We now observe that the number of fixed points of h_i^j on $\Pi^{-1}(y_i)$ is $[N_G(\langle h_i^j \rangle) : \langle h_i \rangle]$.

Lemma 2. *If G is a non-abelian simple group and not of Lie type of rank ≤ 4 or M_{11},M_{12},M_{22},M_{23},J_1, then for every $h \in G$ and every j not a multiple of $|h|$ we have $5 \leq [N_G(\langle h^j \rangle) : \langle h \rangle]$.*

So if G is as in the lemma above and $G = Aut(Y)$ for some compact connected Riemann surface Y, then $S \subset \mathcal{W}(Y)$.

In an ongoing project Helmut Völklein and I are classifying the the pairs (G, X), such that S is not contained $\mathcal{W}(X)$. The group G of such a pair will have at most one non-abelian composition factor. Moreover the derived length of G/G^{∞} and $O(G)$ will be small.

The result below concerning the case of Hurwitz groups [1], which is closely related to the ongoing project shows us what a general result might be.

Theorem 1. *(M.-Völklein) If $|G| = 84(g-1)$, then G acts transitively on $\mathcal{W}(X)$ only if $G \in \{L_2(7), L_2(8), L_2(13)\}$.*

Remarks. Here $\mathcal{W}(X) \subset S$.
If $G = L_2(7)$, then X is the Klein curve. If $G = L_2(8)$, then X is the Macbeath curve. The case $G = L_2(13)$ is open as we do not have an equation for an $L_2(13)$ curve.

References

[1] K. Magaard, H. Völklein, *On Weierstrass points of Hurwitz curves*, J. Algebra **300** (2006), no. 2, 647–654.

Double centralizers of unipotent elements

Donna M. Testerman
(joint work with Ross Lawther)

Let G be a simple algebraic group defined over an algebraically closed field k whose characteristic is either 0 or a good prime for G, and let $u \in G$ be unipotent. We study the centralizer $C_G(u)$, especially its centre $Z(C_G(u))$. In the case where G is of exceptional type we calculate the Lie algebra of $Z(C_G(u))$, in particular determining its dimension.

This work is motivated by the desire to embed u in a connected abelian unipotent subgroup of G satisfying certain uniqueness properties. If $\mathrm{char}(k) = 0$ and $G = SL_n(k)$, for example, one can define such a subgroup as the image of the map $\phi_u : \mathbf{G}_a \to G$, defined by $t \mapsto u^t = \sum_{i\geq 0} \binom{t}{i}(u-1)^i$. It is clear that $C_G(u) = C_G(\mathrm{im}\,\phi_u) = C_G(\mathrm{Lie}(\mathrm{im}\,\phi_u)) = C_G(u-1)$. In [4], Seitz considered this question in the case where either $\mathrm{char}(k) = 0$, or $\mathrm{char}(k)$ is a good prime p for G and u has order p; he constructed a 1-dimensional connected subgroup U of G, intrinsically associated to u, such that $u \in U$ and the centralizers in G of u, the subgroup U and the Lie algebra of U all coincide. In [2], Proud showed that if $\mathrm{char}(k)$ is a good prime p for G, and u has order p^t, then there exists a closed connected t-dimensional abelian unipotent subgroup containing u; however the subgroup satisfies no uniqueness properties. A natural candidate for a canonically defined abelian overgroup of a unipotent element u is $C_G(C_G(u)) = Z(C_G(u))$. In [3], Proud turned to the study of $Z(C_G(u))$, and in particular proved that if $\mathrm{char}(k)$ is either 0 or a good prime for G then $Z(C_G(u)) = Z(G) \times Z(C_G(u))^\circ$ and $Z(C_G(u))^\circ$ is unipotent. Seitz carried this further in [5], showing that $Z(C_G(u))^\circ$ has a decomposition into Witt groups such that u is contained in one (not uniquely determined) factor; he pointed out that while $Z(C_G(u))^\circ$ is 'of considerable interest … even the dimension of this subgroup remains a mystery.' We attempt to shed some light upon this mystery here.

Using the existence of a Springer isomorphism between the varieties of unipotent elements of G and nilpotent elements of its Lie algebra, we replace u by a nilpotent element e for which $C_G(u) = C_G(e)$ and subsequently study $C_G(e)$ and $Z(C_G(e))$.

For the results which follow, we fix the following hypotheses:

- G is a simple algebraic group of exceptional type defined over an algebraically closed field k whose characteristic is either 0 or a good prime for G, and $e \in \mathrm{Lie}(G)$ is nilpotent.
- Let $\tau : k^* \to G$ be a cocharacter associated to e; i.e. $\tau(c)e = c^2e$ for all $c \in k^*$ and $\mathrm{im}(\tau) \subset [L, L]$, where L is the Levi factor of a parabolic subgroup of G such that e is a distinguished nilpotent element in $\mathrm{Lie}([L, L])$. (Recall that e is distinguished in a semisimple group H if $C_H(e)^\circ$ is unipotent.)
- From τ one obtains a unique labelling of the Dynkin diagram of G, with labels taken from the set $\{0, 1, 2\}$; the corresponding labelled diagram Δ is that attached to the G-orbit of e in the Bala-Carter-Pommerening classification of nilpotent

orbits in $\mathrm{Lie}(G)$. We write $n_2(\Delta)$ for the number of labels in Δ which are equal to 2.

Our first result concerns the case where e is distinguished in $\mathrm{Lie}(G)$.

Theorem 1. *Let $d_1 \leqslant \cdots \leqslant d_\ell$ be the degrees of the invariant polynomials of the Weyl group of G. Assume e is distinguished in $\mathrm{Lie}(G)$. Then*
(i) $\dim Z(C_G(e)) = n_2(\Delta) = \dim Z(C_G(\mathrm{im}(\tau)))$; and
(ii) the τ-weights on $\mathrm{Lie}(Z(C_G(e)))$ are the $n_2(\Delta)$ integers $2d_1 - 2, \ldots, 2d_{n_2(\Delta)} - 2$.

Leaving aside the observation about the action of $\mathrm{im}(\tau)$, we may generalize to the case of nilpotent elements whose cocharacters have labelled diagrams with only even labels.

Theorem 2. *Suppose that Δ has no label equal to 1. Then*

$$\dim Z(C_G(e)) = n_2(\Delta) = \dim Z(C_G(\mathrm{im}(\tau))).$$

Theorem 2 is subsumed by a more general result, the statement of which requires the following. Given a labelled diagram Δ for the group G, we define the *2-free core* of Δ to be the sub-labelled diagram Δ_0 obtained by removing from Δ each node whose label is 2. We let G_0 be a semisimple algebraic group (of any isogeny type) defined over k whose Dynkin diagram is the underlying diagram of Δ_0; thus $\operatorname{rank} G_0 = \operatorname{rank} G - n_2(\Delta)$. Note that if $\mathrm{char}(k)$ is positive, it is a good prime for G_0; thus the Bala-Carter-Pommerening classification of nilpotent orbits applies to $\mathrm{Lie}(G_0)$. Indeed, any nilpotent orbit in $\mathrm{Lie}(G_0)$ is a direct product of nilpotent orbits in the simple factors of $\mathrm{Lie}(G_0)$; there is therefore a bijection between the set of nilpotent orbits in $\mathrm{Lie}(G_0)$ and the set of labelled diagrams for G_0 which are unions of labelled diagrams for the simple factors. We then have the following.

Theorem 3. *There exists a nilpotent G_0-orbit in $\mathrm{Lie}(G_0)$ having labelled diagram Δ_0. Let $e_0 \in \mathrm{Lie}(G_0)$ be a representative of this orbit. Then:*
(i) $\dim C_G(e) - \dim C_{G_0}(e_0) = n_2(\Delta)$; and
(ii) $\dim Z(C_G(e)) - \dim Z(C_{G_0}(e_0)) = n_2(\Delta)$.

In fact we have an even more general result on $\dim Z(C_G(e))$. By inspection of the labelled diagrams Δ which occur, we see that Δ_0 always has a connected component with the property that all labels in Δ_0 outside the component are 0.

Theorem 4. *Let $a_1, \ldots, a_\ell$ be the labels of Δ. Then $\dim Z(C_G(e)) = \lceil \frac{1}{2} \sum a_j \rceil + \epsilon$, where $\epsilon \in \{0, \pm 1\}$. Moreover the value of ϵ may be explicitly described as follows. Let Δ_0 be the 2-free core of Δ, with corresponding algebraic group G_0; let Γ_0 be a connected component of Δ_0 such that all labels in $\Delta_0 \setminus \Gamma_0$ are 0, and H_0 be the* *corresponding simple factor of* G_0. *Then* $\epsilon = 0$ *with the following exceptions.*

$\epsilon = 1:$

H_0	Γ_0
F_4	1010
E_7	$\begin{smallmatrix}1&0&1&0&0&0\\&&0\end{smallmatrix}, \begin{smallmatrix}0&0&1&0&1&0\\&&0\end{smallmatrix}$
E_8	$\begin{smallmatrix}0&0&0&0&1&0&1\\&&0\end{smallmatrix}, \begin{smallmatrix}0&1&0&0&0&0&1\\&&0\end{smallmatrix},$ $\begin{smallmatrix}1&0&0&0&1&0&0\\&&0\end{smallmatrix}, \begin{smallmatrix}0&0&1&0&1&0&0\\&&0\end{smallmatrix}$

$\epsilon = -1:$

H_0	Γ_0
D_4	$10\begin{smallmatrix}1\\1\end{smallmatrix}$
D_6	$1000\begin{smallmatrix}1\\1\end{smallmatrix}$
D_7	$10110\begin{smallmatrix}1\\1\end{smallmatrix}$
E_6	$\begin{smallmatrix}1&0&1&0&1\\&&0\end{smallmatrix}, \begin{smallmatrix}1&1&0&1&1\\&&1\end{smallmatrix}$
E_7	$\begin{smallmatrix}1&0&1&0&1&0\\&&0\end{smallmatrix}$
E_8	$\begin{smallmatrix}1&0&0&0&1&0&1\\&&0\end{smallmatrix}, \begin{smallmatrix}1&0&1&0&1&0&0\\&&0\end{smallmatrix}$

We are currently investigating the classical groups and have thus far verified Theorem 3(i) for all types, all of our results (including an analogue of Theorem 4) for type A_ℓ, and Theorem 1 for type C_ℓ. One would like however to find a conceptual proof of the above results, in particular Theorem 1, which was established by Kostant in [1] for the class of regular nilpotent elements.

References

[1] B. Kostant, *The principal three-dimensional subgroup and the Betti numbers of a complex simple Lie group*, Amer. J. Math **81** (1959), 973–1032.

[2] R. Proud, *Witt groups and unipotent elements in algebraic groups*, Proc. London Math. Soc. **82** (2001), 647–675.

[3] R. Proud, *On centralizers of unipotent elements in algebraic groups*, unpublished manuscript.

[4] G.M. Seitz, *Unipotent elements, tilting modules, and saturation*, Invent. Math. **141** (2000), 467–502.

[5] G.M. Seitz, *Unipotent centralizers in algebraic groups*, J. Alg. **279** (2004), 226–259.

On a group-theoretic problem of Gowers

László Pyber
(joint work with N. Nikolov)

A subset X of a group G is called *product-free* if there are no solutions to $xy = z$ with $x, y, z \in X$. The maximal size $\alpha(G)$ of a product-free subset of a finite group G has been considered by Babai and Sós [BS]. For example, they proved that for any soluble group G of order n we have $\alpha(G) \geq \frac{2n}{7}$ and asked whether a similar linear bound holds for arbitrary finite groups.

A negative answer to the above question was obtained very recently by Gowers [Gow]. He showed that for sufficiently large q the group $\Gamma = PSL(2, q)$ has no product-free subsets of size $c|\Gamma|^{\frac{8}{9}}$. His proof depends on the fact, proved by Frobenius, that every non-trivial representation of $PSL(2, q)$ has degree at least $(q-1)/2$.

Gowers proved [Gow, p. 22] the following general result on product-free sets of quasirandom groups.

Proposition 0. *Let G be a group of order n, such that the minimal degree of a nontrivial representation is k. If A, B, C are three subsets of G such that $|A|\,|B|\,|C| > \frac{n^3}{k}$, then there is a triple $(a, b, c) \in A \times B \times C$ such that $ab = c$.* □

The starting point of [NP] is the following surprising consequence.

Corollary 1 ([NP])**.** *Let G be a group of order n, such that the minimal degree of a representation is k. If A, B, C are three subsets of G such that $|A|\,|B|\,|C| > \frac{n^3}{k}$, then we have $A \cdot B \cdot C = G$. In particular, if, say, $|B| > \frac{n}{k^{1/3}}$, then we have $B^3 = G$.*

Corollary 1 apart from its intrinsic interest, seems to be an extremely useful tool. Recently a number of deep theorems have been obtained concerning product decompositions of simple groups. Corollary 1 can be used to give short and relatively elementary proofs, while improving the results.

It is particularly useful in the case of simple groups of Lie type. For these groups rather strong lower bounds on the minimal degree of a representation are known [LS].

As an interesting application we prove the following Waring type theorem. For a group word $w = w(x_1, \dots, x_d)$ let $w(G)$ denote the set of values of w in G.

Theorem 2. *Let $k \geq 1$ and $\overline{w} = \{w_1, \dots, w_k\}$ be a set of non-trivial group words. Let L be a finite simple group of Lie type of rank r over the field $\mathbb{F}_q$ and set $\overline{w}(L) = w_1(L) \cap \dots \cap w_k(L)$. Let W be any subset of $\overline{w}(L)$ such that $|W| \geq |\overline{w}(L)|/q^{r/13}$.*

There exists a positive integer N depending only on $\overline{w}$ such that if $|L| > N$, then we have

$$W^3 = L. \qquad \square$$

As the main result of a difficult paper Shalev [Sh] has obtained the same result in the case $k = 1$ and $W = \overline{w}(L)$ (allowing L to be also an alternating group).[1]

Our proof of Theorem 2 is relatively short compared to [Sh] and uses an auxiliary result from [LSh1]. This says roughly that for simple groups of Lie type not of type A_r or ${}^2A_r$ the sets $\overline{w}(L)$ are "very large".

For groups of type A_r and ${}^2A_r$ we provide somewhat weaker estimates for $|\overline{w}(L)|$ which still make Corollary 1 applicable.

It would be most useful to obtain analogues of Corollary 1 for smaller sets B. The following results indicate how far one can go in this direction.

Theorem 3. *Let G be a finite linear group of degree k over the complex field. Then G has a permutation representation of degree at most c_0k^2 with abelian kernel, where $c_0 < 10^{10}$ is an absolute constant.* □

The proof of this result relies on the Classification of the finite simple groups (CFSG). As an immediate consequence we obtain the following.

[1] We remark that for alternating groups and simple groups of Lie type of bounded rank it was shown later in [LSh1] that in fact one has $\overline{w}(L)^2 = L$ if L is large enough.

Corollary 4. *Let G be a finite group such that G has an irreducible representation of degree $k \geq 2$. Then G has a proper subgroup H of index at most $c_0 k^2$.* □

As a "partial converse" to Proposition 0 Gowers [Gow] proved that if a group G contains no large product-free subsets, then it is quasirandom. More precisely, he gave an elementary argument showing that if the minimal degree of a representation of G is k, then G has a product-free subset of size at least $\frac{n}{c^k}$ for some absolute constant $c > 1$. Gowers asked whether this can be improved to $\frac{n}{k^c}$ (for $k \geq 2$). Applying a result of Kedlaya to H as above we see that G has a product-free subset of size at least $\frac{n}{ck}$ for some constant c, i.e. we obtain a positive answer to his question.

References

[BS] L. Babai and V. T. Sós, *Sidon sets in groups and induced subgraphs of Cayley graphs*, Europ. J. Comb. **6**(1985), 101–114.

[Gow] W. T. Gowers, *Quasirandom groups*, preprint.

[Ke] K. S. Kedlaya, *Product-free subsets of groups*, Amer. Math. Monthly **105**(1998), 900–906.

[LS] V. Landazuri and G. M. Seitz, *On the minimal degrees of projective representations of the finite Chevalley groups*, J. Algebra **32**(1974), 418–443.

[LSh1] M. Larsen and A. Shalev, *Word maps and Waring type problems*, preprint.

[NP] N. Nikolov and L. Pyber, *Product decompositions of quasirandom groups and a Jordan type theorem*, preprint.

[Sh] A. Shalev, *Word maps, conjugacy classes, and a non-commutative Waring-type theorem*, Annals of Math., to appear.

Finite flag-transitive generalized polygons

Hendrik Van Maldeghem

(joint work with Csaba Schneider)

One of the big challenges in the theory of generalized polygons is the classification of flag-transitive generalized polygons. This question only makes sense in the finite case because of the existence of free constructions of flag-transitive generalized n-gons for every $n > 1$ by Jacques Tits in [7].

In the finite case, a celebrated theorem by Feit and Higman [2] heavily restricts the posibilities for n. In fact, finite thick generalized n-gons only exist for $n \in \{2, 3, 4, 6, 8\}$, and the case $n = 2$ (the "generalized digons") is trivial in the sense that every point is incident with every line. So we let digons be digons and assume $n > 2$.

For $n = 3$, work mainly by Kantor has provided a satisfactory "classification". Here, we concentrate on the cases $n = 6, 8$.

In general, flag-transitivity is too weak to guarantee primitivity on the point or line set (of course, the action is always imprimitive on the flags). There exist two nonclassical flag-transitive generalized quadrangles with an imprimitive action on the line set and a primitive action on the point set (these quadrangles are denoted $T^*(O)$ in [4], for O a (projectively unique) transitive hyperoval in the Desarguesian projective plane of order 4 and 16, respectively). Here, we will concentrate on the case where the group acts primitively on both the point and the line set. However, many steps in our proofs and intermediate results only require primitivity on the point or line set, or just flag-transitivity, even sometimes transitivity on the points set is enough.

Our main result is a reduction theorem. We reduce the classification of finite primitive flag-transitive generalized 6- and 8-gons to the almost simple case with socle a Chevalley group.

Theorem. *Let Γ be a finite (thick) generalized n-gon, with $n \in \{6, 8\}$, and suppose that a group G acts faithfully and flag-transitively on Γ. Suppose also that the action of G is primitive on both the point set and the line set of Γ. Then G is an almost simple group with a Chevalley group as socle.*

In the known examples, the Chevalley groups in question are Dickson's groups $\mathsf{G}_2(q)$, the triality groups ${}^3\mathsf{D}_4(q)$ (for $n = 6$) and the twisted group ${}^2\mathsf{F}_4(q)$ (for $q = 2^{2e+1}$, here $n = 8$).

Roughly, our analysis proceeds as follows (see [5]). Quite some O'Nan-Scott classes are ruled out by the observation that, if a group H acts transitively on the point set of Γ, then the centralizer $C_G(H)$ does not act transitively on the point set of Γ.

In projective geometry, involutions play an important role in classification results because their fixed point structure is large and can be explicitly described. In our case, involutions do not have to fix anything — in principle. However, a recent result of Temmermans, Thas and myself [6] states that, if Ω is a generalized m-gon, with $m \in \{4, 6, 8\}$ of order (s, t) (which means that every line carries $s + 1$ points and every point is on $t + 1$ lines), with s and t not relatively prime, then every involution must fix either a point or a line. This observation, together with some other geometric and combinatorial considerations (using known restrictions on the parameters of Γ, for instance), enables us to reduce G to the almost simple case.

If the socle of G is a sporadic group, then transitivity on the point set is already enough to conclude that Γ cannot exist, see [1]. If the socle is an alternating group, then the multiply transitivity of this group in its standard permutation representation is used to kill Γ (usually by constructing a quadrangle in Γ), if the point stabilizer in G is imprimitive or intransitive. In the primitive case, some number theory and estimates, together with a result of Maróti [3] reduce the situation to a finite number of cases. Using a technique developed in [1], all these cases are easily handled.

References

[1] F. Buekenhout & H. Van Maldeghem, Remarks on finite generalized hexagons and octagons with a point transitive automorphism group, **in** *Finite Geometry and Combinatorics*, Proceedings Deinze 1992 (ed. F. De Clerck *et al.*), Cambridge University Press, *London Math. Soc. Lecture Note Ser.* **191**, 89–102.

[2] W. Feit & G. Higman, The nonexistence of certain generalized polygons, *J. Algebra* **1** (1964), 114–131.
[3] A. Maróti, On the orders of primitive groups, *J. Algebra* **258** (2002), 631-640.
[4] S. E. Paybe & J. A. Thas, *Finite Generalized Quadrangles*, Pitman Res. Notes Math. Ser. **110**, London, Boston, Melbourne, 1984.
[5] C. Schneider & H. Van Maldeghem, Primitive flag-transitive generalized hexagons and octagons, *unpublished manuscript.*
[6] B. Temmermans, J. A. Thas & H. Van Maldeghem, On collineations and dualities of finite generalized polygons, *unpublished manuscript.*
[7] J. Tits, Endliche Spiegelungsgruppen, die als Weylgruppen auftreten, *Invent. Math.* **43** (1977), 283–295.

An Aschbacher-O'Nan-Scott type theorem for countable linear groups

Yair Glasner
(joint work with Tsachik Gelander)

All the work mentioned in this note is joint with Tsachik Gelander from the Hebrew University. A reader interested in more details is referred to [GG].

A group action $\Gamma \curvearrowright \Omega$ is called *primitive* if there is no Γ-invariant equivalence relation on the set Ω. Equivalently, primitive actions are transitive, of the form $\Gamma \curvearrowright \Gamma/\Delta$, where Δ is a maximal subgroup. We will say that a group Γ is a *primitive group* if it admits a faithful, primitive action on a set. Whenever we use the word "countable" in this note we will mean infinite and countable.

The Aschbacher-O'Nan-Scott theorem describes the structure of the finite primitive groups. Before describing the classification of the countable primitive linear groups, let us test the waters by describing a few well known examples. The first three mimic well known classes of finite primitive permutation groups, while the fourth does not seem to have a natural finite counterpart.

Example 1. **[Primitive affine groups]** Let M be an infinite vector space over a prime field, namely either $M = \mathbf{F}_p^{\aleph_0}$ or $M = \mathbb{Q}^n$ with $n \in \mathbb{N} \cup \{\infty\}$. Let $\Delta \leqslant \mathrm{GL}(M)$ be such that there are no non-trivial Δ-invariant subgroups of M.

The group $\Gamma = \Delta \ltimes M$ admits a natural *affine* action on M, where M acts on itself by (left) translation, and Δ acts by conjugation. We say that the permutation group $\Gamma \curvearrowright M$ is *primitive of affine type.*

An example of a primitive affine action is the group $\mathbb{Q}^* \ltimes \mathbb{Q}$ with its natural two-transitive action on $\mathbb{Q}$.

Example 2. **[Primitive of diagonal type]** Let M be a nonabelian characteristically simple group, and $\mathrm{Inn}(M) \leqslant \Delta \leqslant \mathrm{Aut}(M)$ a subgroup of $\mathrm{Aut}(M)$ containing $M \cong \mathrm{Inn}(M)$. Assume that there are no non-trivial Δ-invariant subgroups of M. The group $\Gamma = \Delta \ltimes M$ admits a natural affine action on M as above. We say that the permutation group Γ is *primitive of diagonal type*[1].

[1] Note that a group Γ of diagonal type as above, contains another normal subgroup isomorphic to M, namely $\{i(m^{-1})m \mid m \in M\}$ where $i : M \to \mathrm{Inn}(M) < \Delta$ is the natural injection.

Note that in the infinite case a characteristically simple group need not be a product of simple groups. For example the group $\mathrm{Aut}(M) \ltimes M$ where $M = \mathrm{PSL}_n(\mathbf{F}[x])$ will be primitive of diagonal type for every countable field $\mathbf{F}$.

Example 3. **[Classical actions]** Consider the action of the group $\mathrm{PGL}_2(\mathbf{F})$ with its natural 3-transitive action on $\mathbf{P}^1(\mathbf{F})$, where $\mathbf{F}$ is any countable field.

Example 4. It is well known that the free group F_2 admits a faithful, highly transitive action on a countable set. In fact it is not difficult to show that there are uncountably many isomorphism classes of such actions.

The group F_2 in the last example does not seem to fit any of the standard primitive classes that appear in the Aschbacher-O'Nan-Scott theorem. In particular it is definitely not a simple group. The motivation for the theorem below originated in an observation due to myself and Miklós Abért that the existence of primitive actions of F_2 may be accounted for by the fact that F_2 admits many dense embeddings into simple topological groups

Proposition 1. [AG] *Assume that a finitely generated group Γ admits a dense embedding into a simple totally disconnected (polish) topological group. Then Γ is primitive.*

Together with Tsachik Gelander we tried to generalize this result to linear groups that admit a Zariski dense embedding into a simple group. Perhaps surprisingly it turns out that this analysis gives a necessary and sufficient condition for countable linear groups to be primitive.

Theorem 1. **[Main theorem]** *A countable linear group Γ which is not torsion, is primitive if and only if it falls into one of the following, mutually exclusive, categories:*

(i) Γ *is primitive of Affine type,*
(ii) Γ *is primitive of Diagonal type,*
(iii) Γ *admits a linear representation $\rho : \Gamma \to \mathrm{GL}_n(K)$ over an algebraically closed field K where the Zariski closure $G \overset{\mathrm{def}}{=} \overline{\rho(\Gamma)}^Z = H \times H \times \ldots \times H$ is a product of isomorphic, simple center-free algebraic groups and the action of Γ by conjugation is transitive on these simple factors.*

This theorem generalizes the following theorem of Margulis and Soĭfer [MS79, MS81] on the existence of maximal subgroups of infinite index. In fact, the method of proof is strongly influenced by the proof of Margulis and Soĭfer.

Theorem 2. **[Margulis-Soĭfer]** *A finitely generated linear group Γ admits a maximal subgroup of infinite index if and only if it is not virtually solvable.*

Our theorem generalizes the Margulis-Soĭfer theorem in three different ways.

- Margulis and Soĭfer give a necessary and sufficient condition for the existence of a maximal subgroup of infinite index, while we characterize the existence of a maximal subgroup with a trivial core. On the linear part of the equation, the former are characterized by being non virtually solvable, while the latter by the existence of a nearly simple Zariski closure.

- We treat countable groups that need not be finitely generated,
- We proved similar theorems characterizing primitive countable groups in a variety of other geometric settings, including convergence groups, subgroups of mapping class groups of surfaces and groups admitting minimal actions on trees. I refer the reader to our paper in GAFA ([GG]) for a precise statement of all of these results.

Here are two corollaries of our main theorem and of its counterparts.

Corollary 1. [Frattini subgroups] *Let* Γ *be a countable group and* $\phi \overset{\text{def}}{=} \phi(\Gamma)$ *its Frattini subgroup. Then*

- *(c.f. Platonov* [Pla66]*, Wehrfritz* [Weh68]*) If* Γ *is linear in characteristic zero, or if it is finitely generated and linear in positive characteristic then* ϕ *is solvable.*
- *(c.f. Ivanov* [Iva87]*) If* $\Gamma < \mathrm{Mod}(S_g)$ *is a subgroup of the mapping class group of a surface then* ϕ *is solvable.*
- *(c.f. Kapovich* [Kap03]*) If* Γ *is a non-elementary convergence group then* ϕ *is finite and nilpotent.*
- *If* $\Gamma = A *_C B$ *is an amalgamated free product, then* $\phi < C$*.*

The first three items above generalize results of the quoted papers from the setting of finitely generated groups to the setting of countable groups. Note that Platonov and Wehrfritz prove that a finitely generated linear group admits a nilpotent Frattini group — this stronger statement is no longer true for countable linear groups. The last statement answers a question of Higman and Neumann [HN54] (see also [All05]). It was not known previously even for finitely generated groups.

Corollary 2. [Margulis-Soĭfer theorem for countable groups] *A countable linear non-torsion group which is not virtually solvable has a maximal subgroup of infinite index.*

Note that this last corollary is no longer an "if and only if"-statement. Indeed once we allow for groups that are not finitely generated it is possible to have primitive solvable groups, such as the affine group $\mathbb{Q}^* \ltimes \mathbb{Q}$.

Let me finish this report with just a few words about the proof of the main theorem. The necessary condition is easier and uses more or less standard methods. Let Γ be a countable linear primitive group with Zariski closure G. If Γ has a nontrivial intersection with the solvable radical of G, then it admits a normal abelian subgroup; from here it is not difficult to show that it is of affine type. Otherwise we may assume that $G = G_1 \times G_2 \times G_3 \ldots \times G_l$ is semisimple and that it factors as a product of groups satisfying the last condition of the main theorem. If Γ admits two commuting normal subgroups it follows using standard methods that it is of diagonal type. Otherwise Γ injects into one of the G_i factors above and hence satisfies the last condition of the main theorem.

The sufficient condition uses methods that can be traced back to Tits' proof of the Tits alternative [Tit72] and, more recently, to the theorem of Margulis-Soĭfer. Let us assume, for simplicity, that Γ is a linear group with a simple Zariski closure.

Such a group is never virtually solvable, so Tits' alternative implies that it contains a free subgroup. Margulis and Soĭfer establish the existence of a free, profinitely dense subgroup; namely a subgroup that surjects onto every finite quotient of Γ. We go one step further and establish the existence of a free prodense subgroup:

Definition 1. A subgroup $\Delta < \Gamma$ is called *prodense* if it maps onto every proper quotient of Γ. Equivalently Δ is prodense if the permutation action $\Gamma \curvearrowright \Gamma/\Delta$ is quasi-primitive in the sense that every normal subgroup of Γ is transitive.

If $\Delta < \Gamma$ is prodense then any maximal subgroup containing Δ is still prodense and therefore core free. When Γ is finitely generated, the existence of a maximal subgroup $\Delta \leqslant M \leqslant \Gamma$ is a direct consequence of Zorn's lemma; but when Γ is merely countable one has to work harder to construct a prodense subgroup that is contained in a maximal subgroup.

The construction of a prodense subgroup is achieved using dynamical methods. The prodense subgroup $\Delta < \Gamma$ is constructed as a countably generated free group. We guarantee that it is prodense by putting a generator in each coset of every normal subgroup of Γ; Δ remains a proper subgroup in this process because it is free. Finally freeness, or independence of the generators, is obtained by playing a "ping pong" game on a certain projective space $\mathbb{P}^{n-1}(K)$. In order to maintain such a ping pong game, we need a linear representation $\rho : \Gamma \to \mathrm{GL}_n(K)$ in which elements of Γ, as well as its normal subgroups exhibit nice proximal dynamics on the boundary $\mathbb{P}^{n-1}(K)$. It is quite possible that this nice linear representation is not the one that was originally given to us. For example consider the case where $\Gamma < \mathrm{SO}_n(\mathbb{R})$ is contained in a compact group. It may have a simple Zariski closure but its action on the corresponding projective space exhibits no proximal dynamics because it is measure preserving. The ingenious idea of Tits was to overcome this problem using representation theory. For example if Γ above is finitely generated, Tits finds a new representation over some local field where the image of Γ is still not virtually solvable, and the dynamics on the boundary is proximal. In our situation the representation-theoretic problem becomes more complicated. First since the group Γ is no longer finitely generated, it is not possible to obtain nice proximal dynamics over a local field and we need to use valuation fields that are no longer locally compact. Second unlike Margulis and Soĭfer, we are not allowed to use non-faithful representations because we are interested in the existence of faithful permutation representations of Γ. This latter point is where the difference between non-virtually solvable groups and groups with a simple Zariski closure shows up. Finally since the property of being primitive is not a commensurablility invariant, we are not allowed to pass to representations of finite index subgroups. This seemingly innocent-looking problem requires us to work with representations of non-connected algebraic groups, which considerably complicates the proof. Much of the representation theoretic work mentioned above was already dealt with by Breulliard and Gelander in their previous papers [BG03], [BG04].

References

[Pla66] V. P. Platonov. Frattini subgroup of linear groups and finitary approximability. *Dokl. Akad. Nauk SSSR*, 171:798–801, 1966.

[Weh68] B. A. F. Wehrfritz. Frattini subgroups in finitely generated linear groups. *J. London Math. Soc.*, 43:619–622, 1968.

[Iva87] N. V. Ivanov. Subgroups of Teichmüller modular groups and their Frattini subgroups. *Funktsional. Anal. i Prilozhen.*, 21(2):76–77, 1987.

[Kap03] Ilya Kapovich. The Frattini subgroup for subgroups of hyperbolic groups. *J. Group Theorey*, 6(1):115–126, 2003.

[BG03] E. Breuillard and T. Gelander. On dense free subgroups of Lie groups. *J. Algebra*, 261(2):448–467, 2003.

[BG04] E. Breuillard and T. Gelander. Topological tits alternative. To appear in the Annals of Math., 2004.

[HN54] G. Higman and B. H. Neumann. On two questions of Itô. *J. London Math. Soc.*, 29:84–88, 1954.

[AG] Miklós Abért and Yair Glasner. Generic groups acting on regular trees. arXiv:math/0702736v1 [math.GR].

[GG] Tsachik Gelander and Yair Glasner. Countable Primitive Groups. To appear in GAFA. arXiv:math/0503001 [math.GR].

[MS79] G. A. Margulis and G. A. Soĭfer. Nonfree maximal subgroups of infinite index of the group $\mathrm{SL}_n(\mathbf{Z})$. *Uspekhi Mat. Nauk*, 34(4(208)):203–204, 1979.

[MS81] G. A. Margulis and G. A. Soĭfer. Maximal subgroups of infinite index in finitely generated linear groups. *J. Algebra*, 69(1):1–23, 1981.

[Tit72] J. Tits. Free subgroups in linear groups. *J. Algebra*, 20:250–270, 1972.

[All05] R. B. J. T. Allenby. On the upper near Frattini subgroup of a generalized free product. *Houston J. Math.*, 31(4):999–1005 (electronic), 2005.

Sharply 2–transitive sets of permutations

Peter Müller

A set S of permutations on a finite set Ω is said to be sharply transitive if for each $\alpha, \beta \in \Omega$ there is a unique $\sigma \in S$ with $\alpha^\sigma = \beta$. We say S is sharply 2–transitive on Ω if S is sharply transitive on the set of pairs $(\alpha_1, \alpha_2) \in \Omega \times \Omega$ with $\alpha_1 \neq \alpha_2$.

By an old observation of Witt there is a projective plane of order n if and only if there is a sharply 2–transitive set on n points.

By results of Lorimer (see [1] and the references therein) and O'Nan (see [2]) the following was known: Let $G \leq \mathrm{Sym}_n$ be an almost simple 2–transitive permutation group which does not contain Alt_n. Then G contains no sharply 2–transitive set except possibly for $G = M_{11}$, M_{12}, M_{23}, M_{24}, Co_3, or $\mathrm{Sp}_{2m}(2)$ on $2^{2m-1} \pm 2^{m-1}$ points.

We extend O'Nan's character theoretic method into a different direction: Suppose that S is a sharply transitive subset of the permutation group G acting on Ω. For a field K let $M = K[\Omega]$ be the permutation module for G. Let M' be the quotient of M by the principal module $K\sum_{\omega\in\Omega}\omega$, and set $s = \sum_{\sigma\in S}\sigma$, considered as an element of the group ring $K[G]$. By sharp transitivity of S we get that $s(m) = 0$ for all $m \in M'$. Thus s is the 0-map on all compositions factors of M'.

Taking traces one gets the following: Let C_1, C_2, $\dots$, C_h be the conjugacy classes of G. Set $a_i = |S \cap C_i|$. Let χ be the character of a composition factor of M', and let $\chi(C_i)$ be the value $\chi(g)$ for $g \in C_i$. Then $\sum_{i=1}^{h} a_i \chi(C_i) = 0$.

Taking all suitable χ's we get a system of linear equations for the a_i. In some cases one can show the non-existence of S by realizing that this system of equations has no solution with all $a_i \geq 0$. This works for instance for $\mathrm{Sp}_6(2)$ on 28 and 36 points. (Without loss of generality one has $1 \in S$, so $C_1 = \{1\}$ and the classes C_i, $i > 1$, consist of fixed point free permutations.)

One also obtains a contradiction if the characteristic of K does not divide the degree of G, but if the principal module is a composition factor of M'. Using this, one can rule out the remaining symplectic groups and Co_3 by actually showing a stronger result: The point stabilizer of these groups does not contain a set which is sharply transitive on the remaining points.

For Co_3 we use $K = \mathrm{GF}(3)$ and the Brauer atlas, and for the symplectic groups we use $K = \mathrm{GF}(2)$ and results by Sastry and Sin on the characteristic 2 doubly transitive permutation modules of the groups $\mathrm{Sp}_{2m}(2)$.

References

[1] P. Lorimer, *Finite projective planes and sharply 2-transitive subsets of finite groups*, Lecture Notes in Math. **372** (1974), 432–436.

[2] M. E. O'Nan, *Sharply 2-transitive sets of permutations*, Proceedings of the Rutgers group theory year, 1983–1984, Cambridge Univ. Press, Cambridge, 1985, 63–67.

Primitive permutation groups and their section-regular partitions

Peter M. Neumann

Consider a permutation group G acting on a finite set X of size greater than 2. A partition or equivalence relation ρ on X will be said to be *section-regular* for G, or simply *G-regular*, if there is a section (or transversal) S such that S^g is a section of ρ for every g in G; equivalently, S is a section of ρ^g for all $g \in G$. In connection with a question about semigroups that has applications to the study of so-called synchronizing automata, Dr João Araújo (Lisbon) has asked (in an e-mail message of 19 October 2006) the following question. Call G *synchronizing* if it is non-trivial and there are no non-trivial proper G-regular partitions of X. Thus for example any 2-transitive group (indeed any 2-homogeneous group) is synchronizing. It is easy to see that a synchronizing group must be primitive and Dr Araújo asked explicitly whether the converse holds:

Question: *Is every finite primitive permutation group synchronizing?*

The short answer is NO. As usual, however, much lies behind this monosyllable, and that was the subject of this lecture.

The lecture was divided into five parts. The first was introductory and is summarised above. The second contained some analysis. Its main result was the following:

Theorem. *If G is transitive on X and ρ is a section-regular partition for G then ρ is uniform in the sense that all its parts have the same size.*

In light of this result, for a G-regular partition ρ, we define the parameter set (n, r, s) as follows: $n := |X|$, the degree of G; $r := |\rho|$, the size of each ρ-class; and $s := |X/\rho|$, the number of classes of ρ. Clearly, $n = rs$.

As a corollary of the theorem it follows that if G is transitive of prime degree then G is synchronizing. Pushing the analysis a little further one may show that if (n, r, s) is the parameter set of a section-regular partition for a primitive group G then $r > 2$ and $s > 2$; in particular, if G is primitive of degree $2p$, where p is prime, then G is synchronizing.

The third part of the lecture was devoted to a sketch of a number of examples. In particular, from a theorem of D. König (1916; see Philip Hall [1] for references to a number of early proofs) to the effect that two uniform equivalence relations with the same class-sizes always have a common section, it follows that if ρ is an equivalence relation invariant under a subgroup H of index 2 in G then ρ is section-regular for G. There are many primitive groups that have a subgroup of index 2 which is imprimitive, so this provides numerous examples. Others in each of the various classes in the O'Nan–Scott taxonomy of finite primitive groups were described.

The fourth part of the lecture was devoted to exposition of a theorem to the effect that in quite a strong sense primitive non-synchronizing groups are rare. Define E_0 to be the set of natural numbers n for which there exists a primitive group of degree n that is not synchronizing, and define

$$e_0(x) := \big|\{n \in E_0 \mid n \leqslant x\}\big| \,.$$

Thus $e_0(x)$ measures the density of the set E_0.

Theorem. $\quad e_0(x) = (1 + 2^{-\frac{1}{2}})x^{\frac{1}{2}} + O(x^{\frac{1}{2}}/\log x)$.

This is to be compared with the theorem of Cameron, Neumann & Teague [2] which states that if

$$e(x) := \big|\{n \leqslant x \mid \exists G \leqslant \mathrm{Sym}(n),\ G \text{ primitive},\ \mathrm{Alt}(n) \not\leqslant G\,\}\big|$$

then

$$e(x) = 2\pi(x) + (1 + \sqrt{2})x^{\frac{1}{2}} + O(x^{\frac{1}{2}}/\log x)\,,$$

where $\pi(x)$ is the prime-number enumerator. Indeed, the proof of the theorem depends heavily on the proof of that result.

The fifth and concluding part of the lecture offered a number of challenges, such as: to find all G-regular partitions for primitive permutation groups of affine type; to find all primitive non-synchronizing groups of small rank; to find all primitive non-synchronizing groups with section-regular partitions having parameter set $(n, 3, s)$ or $(n, r, 3)$; or, more ambitiously and comprehensively, to classify all primitive non-synchronizing groups and their section-regular partitions. Finally, there is the question what implications the examples, and such a classification, would have for the original questions of Dr Araújo about semigroups and automata.

References

[1] Philip Hall, On representatives of subsets, *J. London Math. Soc.* **10** (1934), 26–30.

[2] Peter J. Cameron, Peter M. Neumann and David N. Teague, On the degrees of primitive permutation groups, *Math. Z.* **180** (1982), 141–149.

Extremely primitive groups

Ákos Seress
(joint work with Avinoam Mann, Cheryl Praeger)

A primitive permutation group is called *extremely primitive* if a point stabilizer acts primitively on each of its orbits. Extremely primitive groups were first considered by Manning [4], who proved that the point stabilizer must act faithfully on all of its nontrivial orbits. We report our efforts toward finding all extremely primitive groups. Proofs will appear in [3].

Our main results are the following.

Theorem 1. *If $G \leq \mathrm{Sym}(\Omega)$ is extremely primitive then G is of affine or almost simple type.*

The bulk of this paper is the further analysis of the affine case. We shall return to the classification of extremely primitive groups of almost simple type in a sequel. The proof of Theorem 1 is independent of the finite simple group classification, but further results rely on this classification: namely Theorem 2 through its use of the classification of finite 2-transitive groups, and Theorems 3, 4 where more detailed information about simple groups and their representations is needed.

Theorem 2. *Let $G \leq \mathrm{Sym}(\Omega)$ be extremely primitive of affine type, so that $|\Omega| = p^d$ for some prime p, $G = NH \leq \mathrm{AGL}\,(d,p)$ with $N = Z_p^d$ and H an irreducible subgroup of $\mathrm{GL}\,(d,p)$. Then one of the following holds.*

- *(a) (soluble examples)*
  - *(i) $d = 1$ and $H = 1$; or*
  - *(ii) $H = Z_q$, where q is a prime, and $o(p \bmod q) = d$; or*
  - *(iii) $H = Z_q.Z_e$, with q as in (ii), and e divides d.*
- *(b) (2-transitive, insoluble examples) $p = 2$ and one of the following holds.*
  - *(i) $H = \mathrm{SL}\,(d,2)$ for $d \geq 3$, or $H = \mathrm{Sp}\,(d,2)$ for $d \geq 4$ even;*
  - *(ii) $(d,H) = (4, A_6)$, $(4, A_7)$, $(6, \mathrm{PSU}\,(3,3))$, $(6, \mathrm{PSU}\,(3,3).2)$.*
- *(c) (insoluble, simply primitive examples) $p = 2$ and H is almost simple.*

Moreover each of the groups in parts (a) and (b) is extremely primitive.

To classify the finite affine extremely primitive groups it remains to find all the examples in part (c) of Theorem 2. This we do up to a finite number of possibilities.

Theorem 3. *For the pairs (d, H) in (a)–(c) below, the group $Z_2^d.H$ is simply primitive and extremely primitive.*

(*a*) $\mathrm{Soc}\,(H)$ *sporadic:* $(10, M_{12})$, $(10, M_{22})$, $(10, M_{22}.2)$, $(11, M_{23})$ *(two groups)*, $(11, M_{24})$ *(two groups)*, $(22, \mathrm{Co}_3)$, $(24, \mathrm{Co}_1)$*;*
(b) $\mathrm{Soc}\,(H)$ *alternating:* $(2k, A_{2k+1})$, $(2k, S_{2k+1})$ *for* $k \geq 2$, $(2k, A_{2k+2})$, $(2k, S_{2k+2})$ *for* $k \geq 3$*;*
(c) $\mathrm{Soc}\,(H)$ *of Lie type:* $(2k, \Omega^{\pm}(2k, 2))$, $(2k, \Omega^{\pm}(2k, 2).2)$ *for* $k \geq 3$, $(8, \mathrm{PSL}\,(2, 17))$, $(8, \mathrm{Sp}\,(6, 2))$.

Moreover, there are only finitely many insoluble, simply primitive, extremely primitive groups of affine type not occurring on this list.

Note that up to permutational isomorphism there are two extremely primitive groups with structure $Z_2^{11}.M_{23}$ and also there are two such groups with structure $Z_2^{11}.M_{24}$. We conjecture that the list in Theorem 3 is complete.

The unknown exceptions in Theorem 3 are due to the fact that we do not have a good bound on the number of maximal subgroups that is valid in *all* almost simple groups. A famous conjecture of G. E. Wall states that the number of maximal subgroups is at most $|H|$ in all groups H. There is recent activity toward proving Wall's conjecture [2], [1] and these results were already used in the proof of Theorem 3. In anticipation of a full proof of Wall's conjecture for almost simple groups, we prove a stronger version of Theorem 3. Let $\mathbf{S}$ be the family of almost simple groups satisfying Wall's conjecture.

Theorem 4. *If $H \in \mathbf{S}$ and $G = Z_2^d.H$ is extremely primitive then either G is listed in Theorems* 2 *or* 3*, or $(d, \mathrm{Soc}\,(H))$ is as in one of the lines of the enclosed table.*

References

[1] M. W. Liebeck, B. M. S. Martin, and A. Shalev, On conjugacy classes of maximal subgroups of finite simple groups, and a related zeta function. *Duke Math. J.* **128** (2005), 541–557.

[2] M. W. Liebeck and A. Shalev, Maximal subgroups of symmetric groups. *J. Combin. Theory Ser. A* **75** (1996), 341–352.

[3] Avinoam Mann, Cheryl E. Praeger, and Ákos Seress, Extremely primitive groups. *Groups, Geometry, and Dynamics*, to appear.

[4] W. A. Manning, Simply transitive primitive groups. *Trans. Amer. Math. Soc.* **29** (1927), 815–825.

d	$\mathrm{Soc}\,(H)$	Conditions
40	$\mathrm{PSp}\,(4,9), \mathrm{SL}\,(5,2)$	two non-permutationally isomorphic groups for $\mathrm{SL}\,(5,2)$
48	$\mathrm{Sp}\,(8,2), \Omega^{\pm}(8,2)$	
70	$\mathrm{SL}\,(8,2), \mathrm{PSU}\,(8,2)$	
100	$\mathrm{Sp}\,(10,2)$	
126	$\mathrm{SL}\,(9,2)$	
$\binom{k}{3}$	$\mathrm{SL}\,(k,2)$	$7 \le k \le 14$
2^k	$\mathrm{Sp}\,(2k,2), \Omega^{+}(2k+2,2)$	$5 \le k \le 8$
27, 78	$\mathrm{E}_6(2)$	
78	${}^2\mathrm{E}_6(2)$	
56, 132	$\mathrm{E}_7(2)$	
248	$\mathrm{E}_8(2)$	

Table 1. Table for Theorem 4.

Counting orbits on subsets and tuples

Peter J. Cameron

Let G be a permutation group on a set Ω, usually infinite (but without loss of generality not larger than countable). Let f_n, F_n, F_n^* denote the numbers of orbits of G on the sets of n-sets, n-tuples of distinct elements, and arbitrary n-tuples from Ω respectively. For given n, if one of these three numbers is finite then all are. The permutation group G is *oligomorphic* if they are finite for all $n \in \mathbb{N}$. We consider the sequences (f_n), (F_n) and (F_n^*), or the corresponding generating functions, where we use the ordinary generating function $\sum f_n x^n$ for f and the exponential generating functions $\sum F_n x^n/n!$, etc., for F and F^*. Let $\mathfrak{f}$, $\mathfrak{F}$ and $\mathfrak{F}^*$ be the sets of all sequences or generating functions arising from oligomorphic groups. Our main problem consists of describing these three sets.

Note that a permutation group on a countable set Ω and its *closure* in the symmetric group on Ω (in the topology of pointwise convergence) have the same orbits on finite subsets and tuples, and so realise the same sequences; so we may assume that G is closed. A permutation group is closed if and only if it is the automorphism group if a first-order structure (which may, without loss, be taken to be a homogeneous relational structure).

Motivation Here are two reasons for being interested in these sequences.

- The automorphism group of a countable first-order structure M is oligomorphic if and only if M is $\aleph_0$-*categorical*, that is, characterised up to isomorphism by countability and its first-order theory (and in this case F^* counts n-types in the first-order theory of M). This was discussed further in Dugald Macpherson's talk.
- Many combinatorial enumeration problems are solved by the sequences f (for unlabelled structures) or F (for labelled structures); precisely, all such problems for *amalgamation classes* (or *Fraïssé classes*).

Products The behaviour of the sequences for direct products (with the intransitive action) and wreath products (with the imprimitive action) are well known: we multiply generating functions in the first case, and substitute in the second (more precisely, if $G = G_1 \operatorname{Wr} G_2$ with the imprimitive action, then $F_G(x) = F_{G_2}(F_{G_1}(x) - 1)$.)

In particular, we have $F_n(S \operatorname{Wr} G) = F_n^*(G)$, so that $\mathfrak{F}^* \subseteq \mathfrak{F}$.

For the product action of the direct product, or the power action of the wreath product, things are more mysterious. Daniele Gewurz, Francesca Merola and I [1] have looked at this.

If $G = G_1 \times G_2$ (with product action), then $F_n^*(G) = F_n^*(G_1)F_n^*(G_2)$. From this one can calculate $F_n(G)$, but there is no nice expression for the generating functions.

If G_2 is a finite permutation group, then $G_1 \operatorname{Wr} G_2$ (in the power action) is oligomorphic, and one can compute $F_n^*(G)$: this is equivalent to counting G_2-orbits on words in an alphabet indexing the G_1-orbits on n-tuples.

We see in particular that $\mathfrak{F}^*$ is closed under pointwise product. Easy examples show that $\mathfrak{F}$ is not. It seems likely that $\mathfrak{F}_{tr}$ and $\mathfrak{F}_{pr}$ (the classes of sequences realised by transitive, resp. primitive oligomorphic groups) are also not closed, but this is not yet known.

Growth rates Much is known but much more is unknown.

Dugald Macpherson showed that there is a constant $c > 1$ such that, if G is oligomorphic and primitive, then either $f_n = 1$ for all n, or $f_n \geq c^n/p(n)$, where p is a polynomial. Macpherson gave $c = \sqrt[5]{2}$.

Recently Francesca Merola [3] improved this to $c = 1.324\ldots$ and also showed that, if G is primitive, either $f_n = 1$ for all n, or $F_n \geq n!c^n/p(n)$.

On the other hand, the smallest known growth for primitive groups has $c = 2$. Known examples of groups with exponential growth are automorphism groups of structures which are "order-like" (linear or circular) or "tree-like", or constructed from such structures by various methods.

This suggests a number of questions. For example:

- Do $\lim_{n\to\infty}(f_n)^{1/n}$ and $\lim_{n\to\infty}(F_n/n!)^{1/n}$ exist?
- What are the possible values of these limits?
- What can be said about groups where the limits are finite?
- Do similar limits such as $\lim_{n\to\infty}(f_n/n!)^{1/n}$ exist?

In all known examples with exponential growth, f_n and $F_n/n!$ are asymptotically of the form $an^{-b}c^n$ for some constants a, b, c. Things are more complicated for growth even slightly beyond exponential. For example, let $G = \operatorname{Sym}(\mathbb{N})$ acting on the set of 2-subsets of $\mathbb{N}$. Thomas Prellberg, Dudley Stark and I [2] have shown that

$$F_n \sim B_{2n} 2^{-n} n^{-1/2} \exp\left(-\left[\frac{1}{2}\log\left(\frac{2n}{\log n}\right)\right]^2\right),$$

where B_{2n} is the *Bell number* (the number of partitions of a $2n$-set).

An algebra Oligomorphic groups give graded algebras.

Let V_n be the vector space of all G-invariant functions from $\binom{\Omega}{n}$ (the set of n-element subsets of Ω) to $\mathbb{C}$. We note that $\dim(V_n) = f_n$ if this is finite.

We make $\mathcal{A} = \bigoplus_{n\geq 0} V_n$ into an algebra by defining, for $\phi \in V_m$, $\psi \in V_n$ and $A \in \binom{\Omega}{m+n}$,

$$(\phi\psi)(A) = \sum_{B\in\binom{A}{m}} \phi(B)\psi(A \setminus B),$$

and extending linearly. Then $\mathcal{A}$ is a commutative and associative graded algebra; if G is oligomorphic then the Hilbert series of $\mathcal{A}$ is the f-series of G. But $\mathcal{A}$ is almost never finitely generated!

Recently Maurice Pouzet [4] has proved an old conjecture of mine: *If G has no finite orbits then $\mathcal{A}$ has no zero-divisors.* The proof involves a novel Ramsey-type theorem. A consequence is that, if G is oligomorphic with no finite orbits then $f_{m+n} \geq f_m + f_n - 1$ for all m, n.

We would like to have other "local" results of this type! These might com from more information about $\mathcal{A}$.

David Glynn has constructed a different algebra on $\bigoplus V_n$ whose multiplication is given by

$$(\phi\psi)(A) = \sum_{B\cup C=A} \phi(B)\psi(C)$$

(so B and C are not required to be disjoint). It is not graded but its structure may be simpler than that of $\mathcal{A}$. (For example, in the finite case, Glynn's algebra is semisimple but mine contains many nilpotent elements.) However, in the case of groups with no finite orbits, I know no examples where the algebras are not isomorphic. The relationship between them is not clear.

References

[1] P. J. Cameron, D. Gewurz and F. Merola, Product action, *Discrete Math.*, in press.

[2] P. J. Cameron, T. Prellberg and D. Stark, Asymptotic enumeration of 2-covers and line graphs, *Discrete Math.*, submitted.

[3] F. Merola, Orbits on n-tuples for infinite permutation groups, *Europ. J. Combinatorics* **22** (2001), 225–241.

[4] M. Pouzet, When the orbit algebra of group is an integral domain? A conjecture of P. J. Cameron, submitted.

Reporter: Guntram Hainke

Participants

Dr. Daniela Amato
Mathematical Institute
24-29 St Giles'
GB-Oxford OX1 1JP

Prof. Dr. Michael Aschbacher
Dept. of Mathematics
California Institute of Technology
Pasadena , CA 91125
USA

Sarah Astill
School of Maths and Statistics
The University of Birmingham
Edgbaston
GB-Birmingham , B15 2TT

Dr. Barbara Baumeister
Institut für Mathematik
Freie Universität Berlin
Arnimallee 2-6
14195 Berlin

Prof. Dr. John van Bon
Dipt. di Matematica
Universita della Calabria
Arvavacata di Rende
I-87036 Rende CS

Prof. Dr. Alexandre Borovik
Department of Mathematics
The University of Manchester
Oxford Road
GB-Manchester M13 9PL

Prof. Dr. Timothy C. Burness
Mathematical Institute
Oxford University
24-29 St. Giles
GB-Oxford OX1 3LB

Prof. Dr. Peter J. Cameron
School of Mathematical Sciences
Queen Mary
University of London
Mile End Road
GB-London E1 4NS

Dr. Pierre-Emmanuel Caprace
Dept. de Mathematiques
Universite Libre de Bruxelles
CP 216 Campus Plaine
Bd. du Triomphe
B-1050 Bruxelles

Prof. Dr. Arjeh M. Cohen
Department of Mathematics and
Computer Science
Eindhoven University of Technology
Postbus 513
NL-5600 MB Eindhoven

David A. Craven
Mathematical Institute
Oxford University
24-29 St. Giles
GB-Oxford OX1 3LB

Dr. Hans Cuypers
Department of Mathematics and
Computer Science
Eindhoven University of Technology
Postbus 513
NL-5600 MB Eindhoven

Erika Damian
Facolta di Ingegneria
Universita di Brescia
Via Valotti 9
I-25060 Brescia

Prof. Dr. Tom De Medts
Dept. of Pure Mathematics and
Computer Algebra
Ghent University
Krijgslaan 281
B-9000 Gent

Prof. Dr. Eloisa Detomi
Dipartimento di Matematica Pura
ed Applicata
Universita di Padova
Via Trieste, 63
I-35121 Padova

Anton Evseev
Magdalen College
Oxford University
GB-Oxford OX1 4AU

Dr. Michael Giudici
School of Mathematics & Statistics
The University of Western Australia
35 Stirling Highway
Crawley 6009 WA
AUSTRALIA

Dr. Yair Glasner
Dept. of Mathematics
Ben-Gurion University of the Negev
Beer Sheva 84 105
ISRAEL

Prof. Dr. Robert M. Guralnick
Department of Mathematics
KAP 108
University of Southern California
3620 S. Vermont Avenue
Los Angeles CA 90089-2532
USA

Dipl.-Math. Guntram Hainke
Fakultät für Mathematik
Universität Bielefeld
Universitätsstr. 25
33615 Bielefeld

Prof. Dr. Jonathan I. Hall
Department of Mathematics
Michigan State University
Wells Hall
East Lansing , MI 48824-1027
USA

Prof. Dr. Gerhard Hiß
Lehrstuhl D für Mathematik
RWTH Aachen
Templergraben 64
52062 Aachen

Prof. Dr. Andrei Jaikin-Zapirain
Departamento de Matematicas
Universidad Autonoma de Madrid
Francisco Tamas y Valiente 7
E-28049 Madrid

Prof. Dr. William M. Kantor
Department of Mathematics
University of Oregon
Eugene , OR 97403-1222
USA

Prof. Dr. Martin Kassabov
Department of Mathematics
Cornell University
310 Malott Hall
Ithaca NY 14853-4201
USA

Dr. Inna Korchagina
Mathematics Institute
University of Warwick
GB-Coventry CV4 7AL

Prof. Dr. Martin W. Liebeck
Department of Mathematics
Imperial College of Science
Technology and Medicine
180 Queen's Gate, Huxley Bldg
GB-London SW7 2BZ

Dr. Andrea Lucchini
Dipartimento di Matematica
Universita di Brescia
Via Valotti, 9
I-25133 Brescia

Prof. Dr. H. Dugald Macpherson
School of Mathematics
University of Leeds
GB-Leeds , LS2 9JT

Prof. Dr. Kay Magaard
Department of Mathematics
Wayne State University
656 West Kirby Avenue
Detroit , MI 48202
USA

Prof. Dr. Hendrik Van Maldeghem
Department of Pure Mathematics and
Computer Algebra
Ghent University
Galglaan 2
B-9000 Gent

Prof. Dr. Gunter Malle
Fachbereich Mathematik
T.U. Kaiserslautern
Erwin-Schrödinger-Straße
67653 Kaiserslautern

Attila Maroti
Department of Mathematics
University of Southern California
3620 South Vermont Ave.,KAP108
Los Angeles , CA 90089-2532
USA

Prof. Dr. Bernhard Mühlherr
Universite Libre de Bruxelles
Service Geometrie
C.P. 216
Bd. du Triomphe
B-1050 Bruxelles

Prof. Dr. Peter Müller
Mathematisches Institut
Universität Würzburg
Am Hubland
97074 Würzburg

Dr. Peter M. Neumann
The Queen's College
Oxford
GB-Oxford OX1 4AW

Hung Ngoc Nguyen
Dept. of Mathematics
University of Florida
358 Little Hall
P.O.Box 118105
Gainesville , FL 32611-8105
USA

Prof. Dr. Cheryl E. Praeger
School of Mathematics & Statistics
The University of Western Australia
35 Stirling Highway
Crawley 6009 WA
AUSTRALIA

Dr. Laszlo Pyber
Alfred Renyi Mathematical Institute
of the Hungarian Academy of Science
Realtanoda u. 13-15
H-1053 Budapest

Jason Rudd
School of Mathematical Sciences
Queen Mary
University of London
Mile End Road
GB-London E1 4NS

Prof. Jan Saxl
Dept. of Pure Mathematics and
Mathematical Statistics
University of Cambridge
Wilberforce Road
GB-Cambridge CB3 OWB

Prof. Dr. Yoav Segev
Dept. of Mathematics
Ben-Gurion University of the Negev
Beer Sheva 84 105
ISRAEL

Prof. Dr. Gary M. Seitz
Department of Mathematics
University of Oregon
Eugene , OR 97403-1222
USA

Prof. Dr. Akos Seress
Department of Mathematics
The Ohio State University
100 Mathematics Building
231 West 18th Avenue
Columbus , OH 43210-1174
USA

Prof. Dr. Aner Shalev
Institute of Mathematics
The Hebrew University
Givat-Ram
91904 Jerusalem
ISRAEL

Prof. Dr. Gernot Stroth
Institut für Mathematik
Naturwissenschaftliche Fakultät III
Universität Halle-Wittenberg
Theodor-Lieser-Str. 5
06120 Halle

Prof. Dr. Katrin Tent
Fakultät für Mathematik
Universität Bielefeld
Postfach 100131
33501 Bielefeld

Prof. Dr. Donna M. Testerman
Ecole Polytechnique Federale de
Lausanne
SB IGAT GR - TE
BCH 3104
CH-1015 Lausanne

Prof. Dr. John Griggs Thompson
Dept. of Mathematics
University of Florida
201, Walker Hall
Gainesville , FL 32611-2082
USA

Prof. Dr. Pham Huu Tiep
Dept. of Mathematics
University of Florida
358 Little Hall
P.O.Box 118105
Gainesville , FL 32611-8105
USA